

ISE

INFORMATION SHARING ENVIRONMENT

**Progress and Plans
Annual Report to The Congress**

Prepared by the
Program Manager, Information Sharing Environment

June 2009

ISE

INFORMATION SHARING ENVIRONMENT

Progress and Plans Annual Report to The Congress

Prepared by the
Program Manager, Information Sharing Environment

June 2009

FOREWORD

MESSAGE FROM THE PROGRAM MANAGER, INFORMATION SHARING ENVIRONMENT

On behalf of the President and the Director of National Intelligence, I am pleased to present this third *Annual Report to the Congress on the Information Sharing Environment* (ISE). It demonstrates real improvements in information sharing by the Office of the Program Manager; Federal agencies; State, local, and tribal governments; and the private sector. The “we” in this report refers to all of these ISE participants.

In the past three years we have created a functioning—but still evolving—ISE that has strengthened our national security. Our goal remains an ISE that shares all information securely and properly among all ISE participants. This requires developing mostly common policies, business processes, and technologies, something that is neither easily nor quickly achieved. Our persistent, cooperative efforts have, however, established a solid foundation of compatible policies and practices, which must continue to evolve unabated for several years to create a fully functional ISE.

Having no template to pattern our efforts on, we invented and designed this foundation—using a general methodology that is apparent throughout the report—to rationalize, simplify, and harmonize existing policies, practices, and technologies drawn from all of our participating agencies and organizations. Indeed, this is our legislative mandate.

The controlled unclassified information framework; the suspicious activity reports initiative; expanded access to classified information by State and urban area fusion centers; an enterprise architecture framework; a common standards program; and comprehensive privacy and civil liberties guidelines are examples of the foundations we have built and the methodology we have developed to allow for secure and proper information sharing among our participating agencies. These are all detailed in this report.

We have accomplished a great deal. Nevertheless, our task is far from finished. The end of the ISE’s foundational phase coincides with the arrival of a new administration and a new phase of ISE implementation. Building on three years’ experience, this report introduces an approach called the ISE Framework—a structured, goal-directed management tool around which we can organize and measure ISE implementation. Along with its associated ISE maturity model, the Framework will better enable both management and stakeholders to establish a fully functional ISE.



Thomas E. McNamara
Program Manager, Information Sharing Environment

TABLE OF CONTENTS

Foreword.....iii

Executive Summaryvii

PART ONE – THE EVOLUTION OF THE ISE: 2005-2008..... 1

The State of the ISE 1

 Background 1

 Why Information Sharing Is Important 1

 The Information Sharing Environment (ISE)..... 2

 Five Communities – Many Stakeholders 3

 What Has Been Accomplished? 4

 Challenges and Priorities 6

PART TWO – ISE PROGRESS AND PLANS: 2008-2009..... 7

Goal 1: Create a Culture of Sharing 7

 1.1 Accountability through Performance Appraisals..... 7

 Background 7

 Progress 7

 Plans 8

 1.2 Training..... 8

 Background 8

 Progress 8

 Plans 9

 1.3 Incentives and Awards 9

 Background 9

 Progress 9

 Plans 9

Goal 2: Reduce Barriers to Sharing.....10

 2.1 Integrated Security Framework..... 10

 Background 10

 Progress 10

 Plans 12

 2.2 Handling of Controlled Unclassified Information 12

 Background 12

 Progress 12

 Plans 13

 2.3 Trusted Sharing Infrastructure 13

 Background 13

 Progress 13

 Plans 14

 2.4 Privacy Protection 14

 Background 14

| | |
|---|-----------|
| Progress | 15 |
| Plans | 16 |
| Goal 3: Improve Sharing Practices with Federal, State, Local, Tribal, and Foreign Partners | 17 |
| 3.1 The Nationwide SAR Initiative..... | 17 |
| Background..... | 17 |
| Progress | 18 |
| Plans | 19 |
| 3.2 State and Major Urban Area Fusion Centers | 20 |
| Background..... | 20 |
| Progress | 21 |
| Plans | 21 |
| 3.3 Improved Production and Dissemination..... | 22 |
| Background..... | 22 |
| Progress | 23 |
| Plans | 24 |
| 3.4 Sharing with Foreign Partners..... | 24 |
| Background..... | 24 |
| Progress | 24 |
| Plans | 24 |
| Goal 4: Institutionalize Sharing | 26 |
| 4.1 ISE Architecture Program | 26 |
| Background..... | 26 |
| Progress | 26 |
| Plans | 27 |
| 4.2 Common Terrorism Information Sharing Standards Program | 28 |
| Background..... | 28 |
| Progress | 28 |
| Plans | 29 |
| PART THREE – MANAGING THE ISE: 2009 AND BEYOND | 31 |
| The Information Sharing Environment Framework..... | 31 |
| Overview..... | 31 |
| The ISE Framework | 32 |
| Linking the ISE Maturity Model to the ISE Framework | 33 |
| The Performance and Investment Integration Process..... | 37 |
| The ISE Maturity Score Card | 39 |
| APPENDICES | 41 |
| Appendix A – ISE Framework | 43 |
| Appendix B – Detailed 2008-2009 ISE Performance Results..... | 49 |
| Appendix C – Acronyms and Abbreviations..... | 59 |

EXECUTIVE SUMMARY

Introduction

This Third Annual Report to the Congress on the Information Sharing Environment (ISE) responds to the requirement in the *Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)*, as amended, for “a progress report on the extent to which the ISE has been implemented.” It reflects the collective accomplishments and challenges of an information sharing partnership between the Program Manager for the Information Sharing Environment (PM-ISE) and a range of Federal and non-Federal partners committed to the continuous improvement of information sharing practices with the overriding goal of increasing our national security while protecting privacy and civil liberties.

Last year’s ISE Annual Report was organized around the response to the Presidential Information Sharing Guidelines and Requirements.¹ It presented performance goals for 2008-09 aligned with four functional areas—*Creating a Culture of Sharing; Reducing Barriers to Sharing; Improving Sharing Practices; and Institutionalizing Sharing*.² These functional areas have become the foundation for the ISE Framework and provide the conceptual basis for this report.

Organization of the Report

This report is organized as follows:

- The **Executive Summary** highlights significant accomplishments since the last report and provides a brief introduction to the ISE Framework.
- **Part One** provides a broad overview of the ISE since its inception.
- **Part Two** describes progress and plans for addressing the four unifying ISE goals—Creating a Culture of Sharing; Reducing Barriers to Sharing; Improving Sharing Practices with Federal, State, Local, Tribal and Foreign Partners; and Institutionalizing Sharing.
- **Part Three** describes the ISE Framework, explains its major features, and shows how it will be used to assess ISE maturity. In addition, Part Three also explains how the ISE will synchronize formerly separate performance and budget management activities into a coordinated approach for demonstrating progress and performance, driving investments, and supporting decision-making on ISE programs.
- The **Appendices** contain more detailed information about important matters that are covered more broadly in the main body of the report, e.g., the ISE Framework and 2008-09 ISE performance results.

¹ *Memorandum to the Heads of Executive Departments and Agencies on the Guidelines and Requirements in Support of the Information Sharing Environment* (December 16, 2005).

² *Annual Report to The Congress on the Information Sharing Environment* (June 2008), pp. 52-53.

GOAL 1: CREATE A CULTURE OF SHARING

Appraisals, Training, and Incentives³

Fostering a culture of sharing is a mandate of both IRTPA and the 2005 Presidential Information Sharing Guidelines and Requirements. It is a long-term effort to change government business practices in the interest of more effective and efficient information sharing among agencies. To accomplish this goal, in 2008-09:

- The Office of Personnel Management (OPM) and the PMI-ISE partnered to produce policy guidance that directed agencies to make information sharing a factor in Federal employees' performance appraisals. This issuance guides agencies in how to develop competency elements regarding the proper sharing of information for use in employee appraisals.
- The PM-ISE released an ISE Core Awareness Training Module to help move Federal agencies from the traditional "need to know" culture to one based on a "responsibility to provide."⁴ The Module provides Federal agencies with a common tool for developing an understanding of the ISE as well as an overview of the Federal Government's counterterrorism and homeland security organizations, systems, and challenges.
- Three-quarters of Federal ISE agencies have now incorporated information sharing into their awards programs. For example, the Department of Defense Chief Information Officer established annual awards that include "information sharing and data management" among criteria for consideration.

GOAL 2: REDUCE BARRIERS TO SHARING

Integrated Security Framework⁵

The PM-ISE—working with the Department of Homeland Security (DHS), the Information Security Oversight Office of the National Archives and Records Administration (NARA), the National Security Council, and other key stakeholders—has begun improving access and management of classified information shared with State, local, and tribal (SLT) and private sector partners by replacing inconsistent policies and processes with a common set of security rules and procedures for handling and safeguarding of classified information. In addition, a number of agencies have taken steps to improve security reciprocity practices. To cite two examples,

- The Director of National Intelligence issued an Intelligence Community Directive that mandates reciprocal acceptance of Information Technology (IT) systems certification and accreditation by all Intelligence Community elements; and
- DHS and the Federal Bureau of Investigation (FBI) published a joint secure space standard that provides a common solution for the installation and certification of facilities that house classified networks at fusion centers.



³ See Section 2.1 for a more detailed discussion of ISE security initiatives.

⁴ See [http://www.ise.gov/docs/Fact_Sheet_ISE_Core_Awareness_Training_FINAL_\(07Aug08\).pdf](http://www.ise.gov/docs/Fact_Sheet_ISE_Core_Awareness_Training_FINAL_(07Aug08).pdf).

⁵ For additional information, see Sections 2.1 and 2.3.

Uniform Marking and Handling of Controlled Unclassified Information⁶

In May 2008, President Bush established a framework for designating, marking, safeguarding, and disseminating Controlled Unclassified Information (CUI), and named NARA as Executive Agent. A CUI Office at NARA, along with an interagency Council, manages and oversees implementation. The Office and Council, in an effort to be completed in 2009, are developing draft CUI policy guidance on: Safeguarding, Dissemination, Dispute Resolution, Marking, Designation, and Information Life Cycle. In May 2009, President Obama established an interagency team to review work completed, and make recommendations on the way ahead.

Implementing Comprehensive Privacy Guidelines⁷

ISE Privacy Guidelines Committee (PGC) members met several times with privacy and civil liberties advocacy groups to listen to and incorporate new ideas into revised ISE policies and processes. The PGC also provided the guidance and tools needed to support the development of privacy and civil liberties policies to be used by Federal and SLT agencies. Specifically, the PGC:

- Published a “Privacy and Civil Liberties Implementation Workbook” to assist Federal agencies with the process of ISE privacy policy development and implementation;
- Completed an ISE Policy Development Tool, ISE Privacy Policy Outline, and a list of Publicly Available Federal Privacy Policies;
- Incorporated ISE Privacy requirements into the *Baseline Capabilities for State and Major Urban Area Fusion Centers*; and
- Provided fusion centers with a privacy policy development template and training on its proper use. The PGC also provided ongoing technical assistance and performed reviews of policy documents. To date, 30 centers have developed and submitted privacy policies.

GOAL 3: IMPROVE SHARING PRACTICES WITH FEDERAL, STATE, LOCAL, TRIBAL, AND FOREIGN PARTNERS

Recognition of the essential role of SLT and private sector partners is fundamental to the ISE and is a critical driver of information sharing in the homeland security and law enforcement communities. This was highlighted in the Executive Order governing U.S. intelligence activities, which was amended in the summer of 2008 to state that

State, local, and tribal governments are critical partners in securing and defending the United States from terrorism and other threats to the United States and its interests. Our national intelligence effort should take into account the responsibilities and requirements of State, local, and tribal governments and, as appropriate, private sector entities, when undertaking the collection and dissemination of information and intelligence to protect the United States.⁸

⁶ See Section 2.2 for a more detailed discussion of CUI.

⁷ See Section 2.4 for a more detailed discussion of ISE privacy activities.

⁸ Executive Order 13470 – further amendments to Executive Order 12333, United States Intelligence Activities (August 1, 2008).

Establishing a Nationwide Suspicious Activity Reporting Initiative⁹

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) is an outgrowth of separate but related activities that respond directly to the mandate in the National Strategy for Information Sharing (NSIS) to establish a “unified process for reporting, tracking, and accessing [SARs]” related to terrorism. The long-term goal is for Federal, State, local, tribal, and law enforcement organizations to participate in a standardized, integrated approach to gathering, documenting, processing, analyzing, and sharing SARs while ensuring that privacy and civil liberties are protected.

In 2008-09, the PM-ISE and its Federal and SLT partners:

- Published an *NSI Concept of Operations (CONOPS)* that describes the NSI process; the requirements that drive it; and the roles, missions, and responsibilities of participating agencies;
- Under the leadership of the Department of Justice’s (DOJ) Bureau of Justice Assistance (BJA), expanded the ISE-SAR Evaluation Environment (EE) to 12 sites, forming a solid foundation for nationwide implementation;
- Fully integrated the FBI’s eGuardian system into the ISE-SAR EE;
- Worked with the PGC to integrate privacy concerns into all levels of the NSI;
- Trained more than 10,000 officers and analysts in the NSI process with emphasis on protecting privacy and civil liberties; and
- Established governance to oversee and recommend how to institutionalize the NSI.

Of particular note, an ISE-SAR EE site was established at the Washington, D.C. Metropolitan Police Department (MPD) to support security before and during the Presidential Inauguration. From late December through Inauguration Day, MPD processed 88 SARs, 16 of which were forwarded to eGuardian as potentially terrorist-related.

Providing a Coordinated Voice to State, Local, and Tribal Governments and the Private Sector¹⁰

The Senior Level Interagency Advisory Group and the National Fusion Center Coordination Group provided leadership, coordination, and guidance to establish a national network of fusion centers with a baseline level capability. Highlights include:

- Publication of the *Baseline Capabilities for State and Major Urban Area Fusion Centers*. This collaborative effort, led by DHS and DOJ, included Federal and SLT agencies and provides benchmarks for assessing fusion center performance;
- Completion of a first-level assessment of 72 centers to evaluate progress against the baseline capabilities and to gather data on current fusion center funding; and
- Deployment of Federal personnel to support fusion center operations. State and local personnel have also been fully integrated into Federal operations such as the FBI’s Joint Terrorism Task Forces, the DHS National Operations Center and the Interagency Threat Assessment and Coordination Group (ITACG) at the National Counterterrorism Center (NCTC).

⁹ For a more detailed discussion of the NSI, see Section 3.1.

¹⁰ See Sections 3.2 and 3.3 for a more detailed discussion of support to State and local governments.

Deployments of classified networks increased in the last year, and access is now available at more than 40 fusion centers. Also, the NCTC and its ITACG improved its Secret level online portal by increasing the number of products posted, expanding SLT awareness of the potential value to their missions, and introducing a new product line— Terrorism Information Sharing Products (TIPS)—specifically tailored to SLT needs.

GOAL 4: INSTITUTIONALIZE SHARING

Creating a Common Information Sharing Architecture¹¹

The ISE Architecture program helps align and create bridges between the diverse systems used by ISE participants to create a more uniform network of interconnected systems. Specifically,

- Version 2 of the *ISE Enterprise Architecture Framework (EAF)* provides technology and systems-wide architecture guidance across the entire ISE community;
- Version 2 of the *ISE Profile and Architecture Implementation Strategy (PAIS)* includes additional implementation guidance for ISE participants on implementing more standard processes, approaches, and techniques; and
- DOJ and DHS have incorporated the ISE EAF into their information sharing segment architectures.

Furthermore, the impact of the ISE EAF extends beyond the ISE. The Office of Management and Budget (OMB) identified the concepts developed in the ISE EAF best practice, and has incorporated them into their *Federal Segment Architecture Methodology*. In addition, other government-wide information sharing initiatives—e.g., the Federal Health Information Sharing Environment and the Maritime Domain Awareness program—have adopted many of the concepts, principles, services, and standards originally developed for the ISE EAF into their architectural developments.

Issuing Common Information Sharing Standards¹²

During 2008-09, the PM-ISE issued a number of new or revised information sharing standards as part of the Common Terrorism Information Sharing Standards Program (CTISS). These issuances included:

- Technical Standards for Information Assurance, Core Transport, and Identity and Access Management for the ISE; and
- An updated ISE-SAR Functional Standard that clarifies implementation guidance on the NSI business process and incorporates stronger privacy protections into ISE-SAR data exchanges. Privacy and civil liberties advocacy groups provided direct input into this standard, helping to strengthen privacy controls and refine terrorism identification criteria to better safeguard First Amendment rights.

¹¹ See Section 4.1 for a more detailed discussion of the ISE Architecture Program.

¹² See Section 4.2 for a more detailed discussion of CTISS.

The Importance of Improving the Management of the ISE¹³

The adoption of the ISE framework and its associated maturity model provides a solid foundation for managing ISE implementation and assessing progress. In addition, the Integrated ISE Investment and Performance Process supplements the Framework with a methodology that uses performance results to drive investments and to allocate resources to the most effective programs and initiatives.

Continued Importance of Information Sharing

This Administration is firmly committed to developing the ISE as envisioned in IRTPA. In a memorandum to Federal agencies, President Obama emphasized that “The global nature of the threats facing the United States requires that our Nation’s entire network of defenders be able rapidly to share ... information so that those who must act have the information they need.” Moreover, the Administration’s Homeland Security agenda is based, in part, on increasing our capacity to share information across all levels of government.¹⁴ This strategy was reaffirmed by Secretary Napolitano at the National Fusion Center Conference in March 2009:

At the Department of Homeland Security, information and intelligence sharing is a top priority and fusion centers play an important role in helping to make that happen, ... In the world we live in today, it’s critical for Federal, State, local and tribal entities to know what the others are doing so each can operate effectively and efficiently. Protecting our country requires a partnership of Federal, State and local resources that are fully integrated to not only gather and analyze information, but then to swiftly share that information with appropriate agencies.¹⁵

This Annual Report should be seen as both an update to the Congress on progress made in designing and implementing the ISE, and as a part of this Administration’s broader effort to improve the way the government manages important information. In the words of the President, we need to “make sure our government is running in the most secure, open, and efficient way possible.”¹⁶

The ISE Framework

The ISE Implementation Plan was designed to guide the ISE through June 2009. Many of the Plan’s 89 actions have been completed—albeit some of them in modified form; others have been changed by the NSIS or subsequent policy direction. It is time, therefore, to close the book on the ISE Implementation Plan actions and adopt a modified approach that will help guide and manage the next phase of ISE implementation. The ISE Framework, while building on the work already done, is a new approach that will drive all future ISE implementation activities. It comprises a set of goals, sub-goals, outcomes, objectives, and activities that constitutes the plan for the next phase of ISE implementation.

In June 2008, the Government Accountability Office (GAO) issued a report on “actions taken to guide the design and implementation of the ISE” and “efforts that have been made to report on progress in implementing the ISE.”¹⁷ While acknowledging the progress made since 2005,

¹³ Part Three discusses both the ISE Framework and the ISE Investment and Performance Process in more detail.

¹⁴ See http://www.whitehouse.gov/agenda/homeland_security/.

¹⁵ Remarks by Homeland Security Secretary Janet Napolitano to the National Fusion Center Conference, Kansas City, MO (March 11, 2009), available at http://www.dhs.gov/ynews/speeches/sp_1236975404263.shtm.

¹⁶ White House Press release, “President Obama Names Vivek Kundra Chief Information Officer” (March 5, 2009).

¹⁷ Information Sharing Environment: Definition of the Results to Be Achieved in Improving Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress, GAO-08-492, (June 2008).

the report concluded that “specific desired outcomes or results should be conceptualized and defined in the planning process ... along with the appropriate projects needed to achieve those results, supporting resources, stakeholder responsibilities, and milestones.” In addition to serving as the successor to the ISE Implementation plan, the ISE Framework responds directly to the recommendations by the GAO. It represents an evolutionary approach that builds on previous ISE implementation management efforts and ties individual ISE products and activities directly to specific objectives, outcomes, sub-goals, and goals, as called for in the GAO report.

The Way Ahead

The progress achieved in implementing the ISE since its inception has continued to move us toward the vision set forth in the ISE Implementation Plan in 2005 of “a trusted partnership among all levels of government in the United States, the private sector, and our foreign partners.” But the work is not yet done. With the adoption of the ISE Framework we now have a management structure in place that will help us not only realize the goals of the ISE as conceived in IRTPA, but will also contribute to the goal of intra- and inter-government collaboration that is integral to the Administration’s Open Government Initiative.¹⁸



18 The Open Government Initiative is discussed at <http://www.whitehouse.gov/open/>.

PART ONE – THE EVOLUTION OF THE ISE: 2005-2008

There has been a recognized need in recent years to enhance national security by establishing an information sharing environment that facilitates the sharing of terrorism-related information ... across agencies and levels of government. The global nature of the threats facing the United States requires that our Nation's entire network of defenders be able rapidly to share ... information so that those who must act have the information they need.

— President Barack H. Obama

THE STATE OF THE ISE

Background

The submission of this report coincides with a number of important transitions, requiring a broader, longer-range look at the ISE than was done in the previous two annual reports.

- First, the new Administration is realigning national and homeland security responsibilities and undertaking new initiatives that depend heavily on effective and efficient information sharing;
- Second, the Program Manager for the Information Sharing Environment (PM-ISE) is transitioning from the ISE Implementation Plan, which has guided the ISE for the last three years, to a modified approach for managing ISE implementation going forward, known as the ISE Framework; and
- Finally, as the ISE enters this new phase of development, it will be called on to support a broader range of participants.

This year, then, is an ideal time for stakeholders to assess what was originally intended, what has already been accomplished, and what remains to be done. This section serves as a prequel to the main body of the report, providing context for stakeholders as they appraise the detailed accomplishments and plans covered more fully in Part Two of the report.

Why Information Sharing Is Important

The term “information sharing” in the ISE context means that the *proper information, properly controlled, gets to the right people in time to counter terrorist threats to our people and institutions*. The 9/11 Commission cited a lack of information sharing as among the “most serious weaknesses” leading to the September 11, 2001 attacks. Since then improved terrorism-related information sharing has been cited as a top policy priority in many independent studies and government strategies (See Figure 1).

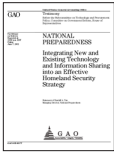


| | 9/11 Commission | Markle Foundation | Government Accountability Office | WMD Commission | National Strategy for Information Sharing |
|-----------------------|--|--|---|---|--|
| |  |  |  |  |  |
| FOCUS | Examined failures in uncovering the 9/11 plot owing to poor information sharing across agency boundaries | Studied the nature of information sharing with an emphasis on decentralized, trusted networks | In several reports, assessed progress toward improving information sharing in intelligence, homeland security, and critical infrastructure | Analyzed the sharing and analysis of intelligence leading up to the second Iraq War | Delivered a fully-coordinated Federal, State, local, and private sector strategy, identifying specific outcomes to improve terrorism-related information sharing |
| MAJOR RECOMMENDATIONS | <ul style="list-style-type: none"> • Provide incentives that promote information sharing • Bring U.S. national security institutions into the information revolution • Create decentralized, trusted information networks across the Federal government | <ul style="list-style-type: none"> • Build a networked community for homeland security • Reduce gaps across Federal agencies and with state and local government and the private sector • Create horizontal information sharing and integration | <ul style="list-style-type: none"> • Information sharing is a “High Risk Area” for the U.S. Government • Improve coordination across information sharing initiatives • Improve Federal-state-local arrangements • Adopt a comprehensive set of performance measures | <ul style="list-style-type: none"> • Create a single focal point for information sharing under DNI • Establish uniform standards and break down policy and technical barriers • Expand sharing of all intelligence, not just terrorist-related information | <ul style="list-style-type: none"> • Foster a culture of awareness • Weave information sharing into all aspects of counterterrorism activity • Implement procedures, processes, and systems that draw upon and integrate existing technical capabilities and established agency authorities |

Figure 1. Perspectives on the ISE

The Information Sharing Environment (ISE)

Both the executive and legislative branches of government have stressed the importance of information sharing as a national priority. Section 1016 of IRTPA called for the establishment of an Information Sharing Environment “for the sharing of terrorism information ... consistent with national security and ... with applicable legal standards relating to privacy and civil liberties.”

Launched formally with the issuance of the ISE Implementation Plan in 2006, the ISE has become:

- The most developed information sharing environment in government;
- The central focal point for terrorism-related information sharing at all government levels; and
- A model for replication of information sharing elsewhere in government.

Building on existing systems and capabilities, the ISE is a system of policies, business practices, architectures, standards, and systems that enable routine, controlled information sharing among all ISE participants. It is *not* a dedicated information system. IRTPA named the ISE an “environment” to suggest decentralized and “mostly common” policies, processes, and standards based on *existing* systems within participating ISE agencies and organizations that collectively support the national counterterrorism (CT) and homeland security (HS) missions.

To “plan for and oversee the implementation of, and manage the ISE,” IIRTPA established the position of Program Manager to be “responsible for information sharing across the Federal Government.”¹⁹ The PM-ISE serves as

- The coordinator of Federal and non-Federal Government, and private sector information sharing;
- The authority for issuing common ISE standards for Federal and non-Federal participants; and
- An “honest broker” to all stakeholders.

Five Communities – Many Stakeholders

Figure 2 shows the ISE as a partnership of five primary communities—Intelligence, Foreign Affairs, Homeland Security, Law Enforcement, and Defense. These communities cut across all levels of government in our Federal system, and include the private sector and foreign partners where appropriate. The purpose of the ISE is to rationalize, standardize, and harmonize the policies, business processes, architectures, standards, and systems used to share information across these communities and among all stakeholders.

To work effectively and efficiently, the ISE must be incorporated into the day-to-day activities, investments, and management processes of all participating ISE agencies and organizations so that it becomes an integral part of their cultures.

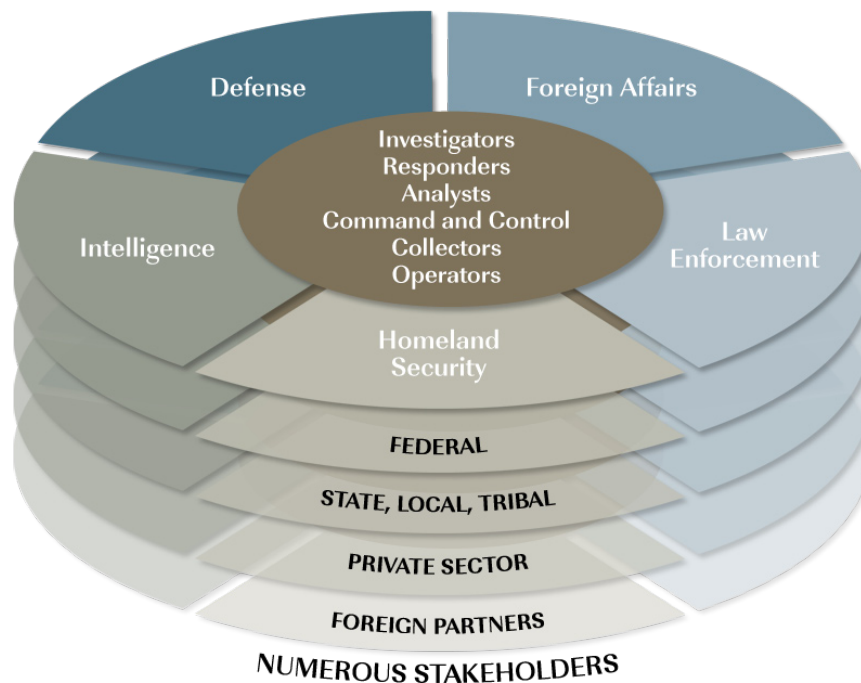


Figure 2. The ISE

¹⁹ IIRTPA §1016(f). Amendments to IIRTPA included in the Implementing Recommendations of the 9/11 Commission Act of 2007 expanded the scope of the ISE, identified additional attributes, and delegated certain authorities, including the authority to issue guidelines and standards, to the PM-ISE.

Although the ISE strives for standardization where possible, clearly these communities have different mission needs and capabilities. State and local processes and policies are not identical to those of the Federal Government, nor will the needs of small towns be the same as those of major urban areas. Thus, the intent is to achieve *mostly common* capabilities—based on common frameworks supported by *mostly common* laws, regulations, policies, business practices, architectures, standards, and systems—tailored as needed to individual participant needs. ISE capabilities, therefore, are being developed with input from all levels of government as well as the private sector.

What Has Been Accomplished?

The ISE reflects a commitment at all levels and branches of government to remove barriers to and to adopt best practices for information sharing.

Four years after IRTPA, some of the most significant barriers to Federal, State, local, tribal, and private sector information sharing have fallen. The **six major accomplishments** highlighted below demonstrate and explain the progress that has been made among all ISE participants, cutting across agencies and communities of interest.

1. Establishment of a Framework for Improved Information Sharing with State, Local, and Tribal Governments, and the Private Sector

The PM-ISE has ensured that the needs and requirements of State, local, and tribal governments, and private sector partners, are fully integrated into national planning efforts for the ISE. Specifically, the Program Manager has led efforts to:

- Place State and local law enforcement officials in the National Counter Terrorism Center (NCTC);
- Establish a national network of State and major urban area fusion centers; and
- Enable sharing of suspicious activities reports across all levels of government through the nationwide Suspicious Activity Reporting (SAR) process.

2. Issuance of Comprehensive Privacy Guidelines

The ISE Privacy Guidelines require agencies to implement policies and processes to better protect privacy. The Guidelines provide top level guidance on important privacy topics such as redress; notice mechanisms; data quality; data security; and accountability, enforcement, and audit mechanisms. Implementing guidelines and tools have been issued over the last several years that provide more specific guidance. Implementation of these guidelines is the responsibility of an interagency Privacy Guidelines Committee (PGC) comprised of senior Federal Privacy Officials who ensure that the ISE incorporates protections for the privacy rights and civil liberties of individuals.

3. Creation of a Standardized Framework for Controlled Unclassified Information

The PM-ISE led a broad-based effort that established a government-wide policy framework that eliminates more than 100 marking and handling policies to better protect and share Controlled Unclassified Information (CUI)—formerly known as Sensitive But Unclassified (SBU) information.²⁰ State, local, and tribal (SLT) and private sector representatives participated with Federal partners in creating this policy framework.

²⁰ One reason for adopting the term CUI was that ‘SBU’ was used in two ways. In addition to being a

4. Development of a Decentralized, Information Sharing Architecture Framework

In 2007, the PM-ISE released the first government-wide ISE Enterprise Architecture Framework. This Framework provides specific guidance to Chief Technology Officers so that ISE technology planning is incorporated into the government-wide Federal Enterprise Architecture for long-term viability of information sharing capabilities and investments. This will ensure that uniform capabilities are built into participating ISE systems to enable connectivity, interoperability, and seamless information sharing.

5. Issuance of Common Terrorism Information Sharing Standards

Common Standards are the fundamental building blocks of the ISE. Recognizing this, the PM-ISE established a government-wide program to develop standards that enable broad Federal access, distribution, and sharing. These standards also improve sharing with State and local partners. This effort is critical to ensure that Federal, State, and local investments for technology development are compatible and that they support information sharing requirements at all levels of government.

6. Promotion and Fostering of a Culture of Sharing

Organizational and community cultures across the ISE vary widely, and information sharing is not always viewed as a required—or even desired—behavior. To create awareness of the importance of appropriate information sharing, to promote such behavior, and to foster a common understanding of the ISE, the PM-ISE issued an “ISE 101” training course in the summer of 2008. Federal agencies have already instituted extensive training about information sharing and are incorporating this course into their training programs. Other ISE participants will use it as the foundation for organization-specific training.

The PM-ISE partnered with the Office of Personnel Management (OPM) to issue guidance for including the appropriate sharing of information as an element in employee performance appraisals. Agencies will be assessed on their success in implementing this guidance through the ISE Performance Management Program.

“ISE 101,” the revised standards for performance evaluations, and agency incentive programs, are all designed to change the traditional “need to know” culture that exists in many participating agencies into cultures that are based on a “responsibility to provide.”

Challenges and Priorities

These accomplishments notwithstanding, the breadth and complexity of the challenges to effective and efficient information-sharing remain formidable. Differing missions, overlapping “turf” conflicts, resource shortfalls, bureaucratic inertia, and agency “tunnel vision” still exist and impede information sharing among ISE participants.

Cultural change remains the most difficult hurdle of all. To bring the ISE to maturity, a number of challenges need to be addressed at all levels of government and with our private sector partners. The following list highlights some of these:

- **Institutionalize the Nationwide Suspicious Activity Reporting Initiative (NSI).** We need to institutionalize a nationwide capability to gather and share SAR information in a

generic description of the type of information, it was also one of the specific markings used.

manner that facilitates the maintenance of national security while continuing to protect privacy rights and civil liberties.

- **Improve Support to Federal, State, Local, and Tribal Partners.** This includes: ensuring that fusion centers and other State and local agencies have access to the classified and unclassified Federal information they need; increasing the flow of fusion center information and analyses to other SLT agencies and the Federal Government; and examining long-term sustainability issues regarding State and major urban area Fusion Centers so that they operate at a baseline level of capabilities.
- **Implement the CUI Framework.** Fully implement policies and processes in accordance with the CUI Registry (to include technology and training initiatives) to support agencies' transition to the CUI Framework.
- **Protect Privacy and Civil Liberties.** Institutionalize Federal privacy policies, incorporate ISE privacy requirements in agency training, and encourage States to implement mostly common privacy policies equivalent to those of the Federal Government.
- **Reduce Improper Classification to Enhance Information Sharing.** Eliminate "need to know" requirements and protocols, and minimize the effect of excessive originator controls on the ability to discover and share information.
- **Improve ISE Security.** Adopt common standards and processes for security clearances, identity management, and role-based access to improve controlled sharing among all ISE participants.
- **Implement Reciprocity Policies and Practices for Clearances, Systems, and Facilities.** Align Federal security policy regarding facilities, personnel, and information technology (IT) systems, and adopt the principle of security reciprocity in all Federal agencies and with SLT and private sector partners
- **Coordinate Investments for Terrorism-Related Initiatives.** Track agency budgets, reduce overlaps and gaps in funding, and monitor investments in order to drive agencies to use compatible technologies and business processes and to maximize the use of scarce resources.

The Obama Administration will continue to make trusted and resilient information sharing and access a top priority and has initiated a comprehensive review of information sharing within the Executive Branch, to include the current status of efforts to establish the ISE. This review of information sharing policies and capabilities will be led by the Senior Director for Information Sharing Policy within the Executive Office of the President's National Security Staff. The Office of the PM-ISE will work closely with the Senior Director in conducting this review and in formulating and implementing the Administration's information sharing policies on an ongoing basis. Additionally, the Senior Director will be supported by staff from the Office of Management and Budget who will review information sharing policies, with particular emphasis on government-wide standards and architecture. Over the next several months, the ongoing review will seek input from Federal, State, local, tribal, and private sector partners to identify and prioritize achievable goals. Consistent with the President's direction, the Information Sharing Council will be integrated into the White House chaired Information Sharing and Access Interagency Policy Committee.

PART TWO – ISE PROGRESS AND PLANS: 2008-2009

The President is committed to securing the homeland against 21st century threats by preventing terrorist attacks and other threats against our homeland, preparing and planning for emergencies, and investing in strong response and recovery capabilities. We will help ensure that the Federal Government works with states and local governments, and the private sector, as close partners in a national approach to prevention, mitigation, and response.

— White House Statement on Homeland Security

GOAL 1: CREATE A CULTURE OF SHARING

Establish employee behaviors, including awareness of information sharing policies, responsibility to perform information sharing activities, and accountability and incentives for carrying out those responsibilities.

1
GOAL

1.1 Accountability through Performance Appraisals

Background

The effort to foster a culture of information sharing at ISE agencies traces its origins to IRTPA and the Presidential Information Sharing Guidelines and Requirements of 2005.²¹

Creating a culture of sharing requires changing traditional patterns of behavior by establishing, reinforcing, and rewarding new behaviors. The Government's performance appraisal systems are important tools for achieving this kind of change. Making appropriate information sharing a factor in performance appraisals will help instill a predisposition to share among employees.

Progress

In 2008-09, the PM-ISE, working with OPM and the Chief Human Capital Offices, took concrete actions to foster a sharing culture:

- OPM endorsed PM-ISE policy guidance that directed agencies to make information sharing a factor in the performance appraisals of Federal employees. This Guidance advises agencies on mandatory and suggested elements of information sharing competency, and includes sample performance appraisal narratives.²²

²¹ See IRTPA (as amended) §1016(d)(3). This direction was later amplified by a Presidential memorandum, "Guidelines and Requirements in Support of the Information Sharing Environment" (December 16, 2005), paragraph 3.

²² "Inclusion of Information Sharing Performance Evaluation Element In Employee Performance Appraisals", ISE-G-105 (September 2008) located at http://www.ise.gov/docs/guidance/ISE-G-105_Inclusion_of_Information_Sharing_Perf_Evaluation-web.pdf.

1 GOAL

- PM-ISE worked with OPM to ensure that this Guidance was aligned with the criteria in the Performance Appraisal Assessment Tool, which supports the effort to achieve a results-oriented performance culture.

.....
APPRAISALS

As of spring 2009, 87% of Federal ISE agencies have taken steps to include information sharing in their performance appraisals.

More than 17,000 Federal Bureau of Investigation (FBI) employees are being evaluated on how well they share information.
.....

Plans

The PM-ISE will work with OPM, the Chief Human Capital Officers’ Council, and agency human resource staff to ensure the successful implementation of the guidance, and will work with ISC agencies to ensure that information sharing is recognized as a leadership imperative and that it is eventually institutionalized throughout the Federal Government.

1.2 Training

Background

Training is a fundamental part of changing organizational culture. This area of effort focuses on encouraging and reinforcing a predisposition to share by training personnel to carry out their information sharing responsibilities.

Progress

In July 2008, the PM-ISE released the Information Sharing Environment Core Awareness Training Module.”²³ This Module provides a common understanding of the ISE and an overview of the Government’s counterterrorism organizations, systems, and challenges.

As part of the ISE-SAR Evaluation Environment (EE), the PM-ISE and its partners require all participants to complete introductory training to ensure that the process of gathering, analyzing, and sharing SARs is conducted in a way that protects privacy and civil liberties.

.....
TRAINING

More than 15,000 personnel have completed the ISE Core Awareness Training Course.

As of April 2009, 73% of agencies had plans in place to implement the Core Awareness Training.
.....

This ISE EE training provides employees with the knowledge and skills needed to help *front-line officers* identify suspicious behaviors relevant to terrorist activity; *analysts* to understand how to identify potential terrorism threats before they become attacks; and *executives* to ensure that management supports the operational implementation of the SAR process, and that privacy and civil liberties are protected throughout the process.

 23 See [http://www.ise.gov/docs/Fact_Sheet_ISE_Core_Awareness_Training_FINAL_\(07Aug08\).pdf](http://www.ise.gov/docs/Fact_Sheet_ISE_Core_Awareness_Training_FINAL_(07Aug08).pdf).

Plans

During 2009-10, the PM-ISE will work with agency training staffs to ensure comprehensive implementation of the ISE Core Awareness Module into all participating agencies and organizations. In addition, the PM-ISE plans to develop a cross-government catalog of information sharing resources for its website (www.ise.gov) to facilitate the sharing of training opportunities and to allow agencies to capitalize on training investments across the Federal Government. Plans are also underway to incorporate SAR training into established law enforcement training programs, such as the basic curriculum of the Federal Law Enforcement Training Center, a component of the Department of Homeland Security (DHS).



1
GOAL

1.3 Incentives and Awards

Background

Incentives and awards form the third element of the strategy for fostering an information sharing culture. This area concentrates on highlighting the crucial importance of information sharing by rewarding those who incorporate sharing behavior into their day-to-day work.

Progress

Almost three quarters of Federal agencies have already adopted or are committed to adopting incentives to information sharing as part of their awards programs. For example, the FBI has implemented a “Chief Information Sharing Officer Award” to enhance awareness of information-sharing goals and the central role they play in the FBI’s national security and criminal mission. Also, the Department of Defense (DoD) Chief Information Officer has established an annual awards program that includes “information sharing and data management” as criteria for awards.

Plans

The PM-ISE is developing a broader array of incentive programs for consideration in the 2009-10 timeframe. In addition, recognition of employees for excellence in collaboration and information sharing across agencies is an important element in making interagency information sharing a part of the culture of ISE participants.

2
GOAL

GOAL 2: REDUCE BARRIERS TO SHARING

Use policy, business process and practices, and technology to remove obstacles and enable information sharing.

2.1 Integrated Security Framework

Background

Defending the Nation against 21st century threats depends on sharing information—both classified and unclassified—with State, local, and tribal officials, law enforcement officers, other first responders, and private sector organizations. All too often, however, cumbersome or inconsistent policies and procedures restrict such sharing, hindering law enforcement officers and other first responders in carrying out their CT and HS responsibilities.

To address this problem, the Classified Domain Working Group (CDWG), chaired by the DHS, has recommended the development of a management framework that would provide uniform and consistent standards for sharing and safeguarding classified information with SLT and private sector partners.

.....
SECURITY RECIPROCITY

93% of ISE agencies now recognize background investigations and adjudications completed by other agencies; 80% recognize other agencies' facilities accreditation processes.
.....

Reciprocity of IT system security certification and the acceptance and recognition among participating ISE agencies of each other's accreditation decisions is another important factor in ensuring efficient and effective information sharing. Several initiatives—led jointly by the National Institutes of Standards and Technology, the Committee on National Security Systems, and the Office of the Director of National Intelligence (ODNI)—have made considerable progress in updating IT security policies and standards. These organizations continue to work together to coordinate policies and standards in an effort to move towards a unified baseline of Federal systems in the ISE as well as to enable reciprocity with SLT governments and private sector partners.

In May 2009, President Obama directed the Assistant to the President for National Security Affairs to review Executive Order 12958 as amended, and to submit recommendations for proposed revisions provide for greater openness and transparency in the Government's security classification and declassification program.²⁴

Progress

Using the CDWG recommendation as a starting point, the PM-ISE, with DHS, the Information Security Oversight Office of the National Archives and Records Administration (NARA), the National Security Council, and other key stakeholders, has begun to explore ways to remove impediments to full State and local participation in the ISE. The intent is to establish a policy framework and management structure for safeguarding classified information shared with SLT and private sector partners.

²⁴ "Memorandum for the Heads of Executive Departments and Agencies, Subject: Classified Information and Controlled Unclassified Information" (May 27, 2009), Section 1(b).

This effort (See Figure 3), which could be structured on the National Industrial Security Program model, will support the significant progress made during 2008-09 in reducing barriers to sharing information among Federal agencies and State, local, and tribal partners. These efforts have included:

- Establishment of a Joint Security and Suitability Reform Team by the DNI, OPM, and the Office of Management and Budget (OMB) to develop uniform policies and procedures to ensure the effective, efficient, and timely completion of security clearances and determinations;
- Issuance of Executive Order 13467, which mandates the alignment of suitability and security clearance processes, establishes a governance structure and Performance Accountability Council, and designates the DNI as Security Executive Agent;
- Issuance of Executive Order 13488, which mandates reciprocal recognition of prior favorable fitness or suitability determinations when based on OPM criteria;²⁵
- Approval of Federal Investigative Standards to support a more streamlined and efficient investigative process, with each successively higher level of investigation building upon—but not duplicating—the ones below;
- DNI Issuance of Intelligence Community Directive 503, which mandates reciprocal acceptance of IT systems certification and accreditation for all Intelligence Community elements; and
- DHS and FBI adoption of a Reciprocal Physical Security Construction Standard that has created an environment where classified information may be stored, used, discussed, or processed. (These two agencies have also developed a reciprocal security construction standard for federally-sponsored SLT secure areas.)

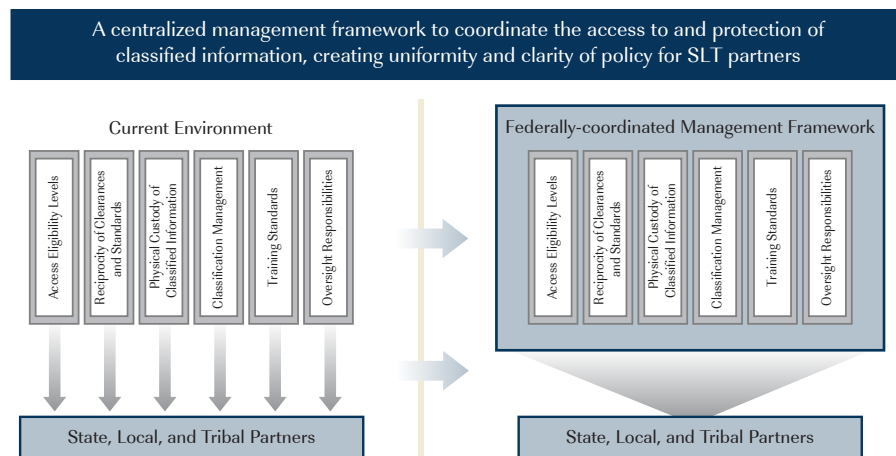


Figure 3. Conceptual View of Integrated Security Framework



²⁵ Executive Order 13467 can be found at <http://www.gpo.gov/fdsys/pkg/WCPD-2008-07-07/pdf/WCPD-2008-07-07-Pg932.pdf>; Executive Order 13488 at <http://www.archives.gov/federal-register/executive-orders/2009-wbush.html>.

2 GOAL

Plans

The PM-ISE will work with key Federal agencies and SLT partners to develop a centralized security management framework for sharing classified information with all ISE partners. In addition, Federal ISE participants will actively engage in the Presidentially-directed review of the processes used in the Government's classification and declassification programs.

2.2 Handling of Controlled Unclassified Information

Background

The sharing of SBU information is currently governed by a bewildering array of policies and practices that confuse both those who produce such information and those who use it in their daily work. Across the Federal Government today, more than 100 unique SBU markings and more than 130 different labeling or handling processes and procedures are in use. The result is an unmanageable collection of SBU rules and sharing practices that impede the proper flow of information between Federal, SLT, and private sector partners.


To address this problem, in May 2008 President Bush established a new CUI Framework for "designating, marking, safeguarding, and disseminating information designated as CUI," and named NARA as Executive Agent.²⁶ In response to the Presidential Memorandum calling for this new Framework, the Archivist of the United States established the CUI Office and appointed a Director to oversee and manage its implementation.

In a memorandum dated May 27, 2009, President Obama directed the Attorney General and the Secretary of Homeland Security to lead an interagency task force on CUI "to review current procedures for categorizing and sharing SBU information to determine whether such procedures strike the proper balance among the relevant imperatives ... These imperatives include protecting legitimate security, law enforcement, and privacy interests as well as civil liberties, providing clear rules to those who handle SBU information, and ensuring that the handling and dissemination of information is not restricted unless there is a compelling need."²⁷

Progress

The CUI Office has committed to a timeline for implementation of the CUI Framework that emphasizes early development of key elements such as policy and processes, a CUI Registry, and a training program.

The May 2008 Presidential Memorandum also established an interagency council to advise NARA on the implementation of the CUI Framework. The CUI Office, in consultation with the Council, is developing draft guidance in several key policy areas to include: Safeguarding, Dissemination, Dispute Resolution, Marking, Designation, and Information Life Cycle.

 To increase awareness of its efforts, the CUI Office has established a website at www.archives.gov/cui; has developed outreach products for stakeholders; and has made presentations to and participated in panel discussions with Federal, State, local, and private sector entities and other stakeholders. Officials from NARA have also met with key public advocacy and privacy partners to better understand and address their concerns with regard to implementation of the Framework.

²⁶ "Memorandum for the Heads of Executive Departments and Agencies on the Designation and Sharing of Controlled Unclassified Information (CUI)" (May 9, 2008)

²⁷ "Memorandum for the Heads of executive Departments and Agencies, Subject: Classified Information and Controlled Unclassified Information" (May 27, 2009), Section 2(b).

Plans

The CUI Office will implement the CUI Registry—an online communications tool that will relay policy updates electronically to the broad ISE stakeholder community. When completed, the approved policy guidance will be submitted into the Federal regulatory process for comment and review by the interagency and the public. Agency implementation is expected to begin in 2011; full implementation of the CUI Framework is required by 2013.

The CUI Office is also developing a training and awareness program aimed at both general and specialized stakeholder audiences at all levels of government. In addition, the CUI Office and Council will support the efforts of the interagency CUI task force established in the May 27, 2009 Presidential Memorandum.

2.3 Trusted Sharing Infrastructure

Background

The term “ISE Shared Spaces”—a key element of the ISE Enterprise Architecture Framework (EAF)—describes a functional concept rather than a specific implementation of technology. The ISE Shared Spaces concept, illustrated in Figure 4, helps address the information processing and usage requirements in IRTPA by employing a structured, standards-based, and distributed approach to information sharing.²⁸ ISE participants use these trusted information repositories to:

- Make standardized terrorism-related information, applications, and services accessible to other ISE participants;
- Store and share information, consistent with the requirements of privacy and civil liberty protections;
- Allow ISE participants operating on national security system (NSS) networks to freely exchange information with participants on non-NSS networks; and
- Provide the means for foreign partners to interface with and share terrorism-related information with U.S. counterparts.

Progress

Highlights of Trusted Sharing Infrastructure efforts during 2008-09 include:

- The Washington, D.C. Metropolitan Police Department (MPD) ISE Shared Space implementation linked the Department’s Alert Management System, containing MPD SAR information, to their new ISE Shared Space. The MPD used its ISE Shared Space and eGuardian interfaces to share ISE-SARs with other law enforcement agencies during the 2009 Presidential Inauguration.
- Seven fusion centers have received ISE Shared Spaces hardware, network, and software applications, as part of the ISE-SAR Evaluation Environment (EE). Work continues in interconnecting these systems and their supporting networks through a federated, secure web page.

²⁸ For additional information on ISE Shared Spaces, see *Information Sharing Environment Enterprise Architecture Framework, Version 2.0* (September 2008), pp. 61-63.

2
GOAL

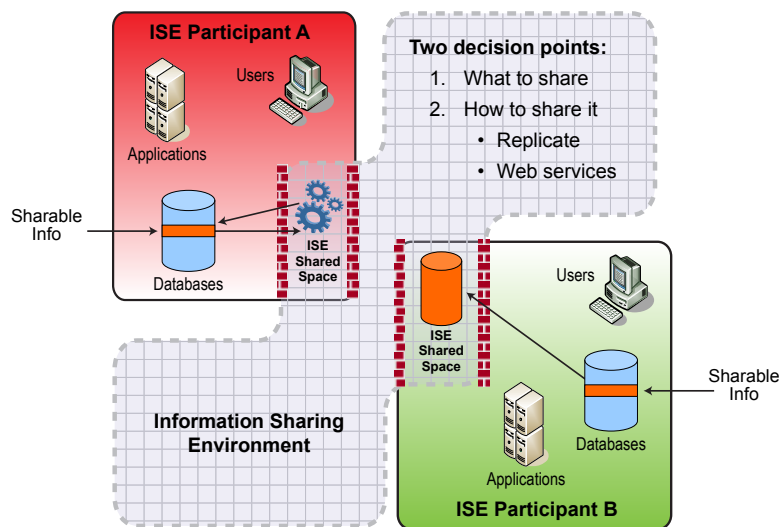


Figure 4. ISE Shared Spaces Concept

Plans

The PM-ISE, the Department of Justice’s (DOJ) Bureau of Justice Assistance (BJA), and SLT partners will continue the installation and activation of ISE Shared Spaces at fusion centers in Houston, Seattle, Los Angeles, and Las Vegas. Federal agencies will implement ISE Shared Spaces as part of the ISE-SAR EE and begin to implement other ISE Shared Space solutions consistent with PM-ISE architectural direction and FY 2010-14 ISE Programmatic Guidance. The PM-ISE will also continue to support the convergence of IT systems security standards and the streamlining of processes for reciprocity. This in turn will support effective and efficient interconnection between all ISE partner organizations.

2.4 Privacy Protection

Background

Protecting privacy, civil rights, and civil liberties is a major requirement in IRTPA and a core attribute of the ISE.²⁹ As required by IRTPA, ISE Privacy Guidelines were developed by an interagency team and approved by the President in November 2006.³⁰ To assist agencies in implementing the ISE Privacy Guidelines, additional guidance documents, including a “Privacy and Civil Liberties Implementation Workbook,” were developed.³¹ The Workbook provides a step-by-step approach to developing ISE privacy, civil rights, and civil liberties policies for Federal agencies and also serves as a resource to SLT agencies and other ISE participants in creating their own privacy policies.

²⁹ IRTPA (as amended) § 1016(b)(2)(H).

³⁰ The ISE Privacy Guidelines, formally entitled “Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment” can be found on the PM-ISE website, www.ise.gov.

³¹ The Workbook and other implementation guidance documents are also located at www.ise.gov.

Progress

During 2008-09, the ISE Privacy Guidelines Committee (PGC) has focused on the development and implementation of ISE privacy, civil rights, and civil liberties policies for ISE member Federal agencies (See Figure 5).

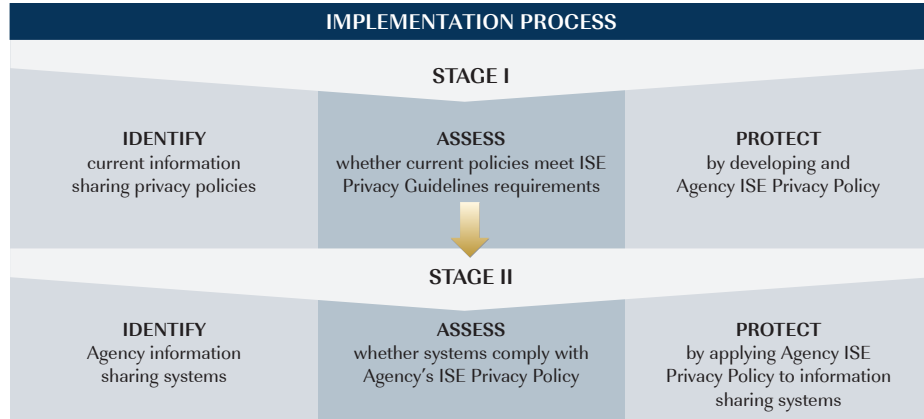


Figure 5. Implementation of ISE Privacy Guidelines

The actions taken by the PGC have helped participating Federal agencies, as well as non-Federal entities, particularly State and major urban area fusion centers.

Specifically, the PGC:

- Published the “Privacy and Civil Liberties Implementation Workbook” to assist Federal agencies with the process of developing and implementing ISE privacy policy as outlined in the ISE Privacy Guidelines;
- Developed and released tools to supplement the Workbook, including an ISE *Policy Development Tool*, *ISE Privacy Policy Outline*, and a list of Publicly Available Federal Privacy Policies;
- In conjunction with the Global Justice Information Sharing Initiative, incorporated ISE Privacy Guidelines compliance requirements into the Baseline Capabilities for State and Major Urban Area Fusion Centers;

.....
FUSION CENTER PRIVACY POLICIES
.....

The Baseline Capabilities require each fusion center to publish a center-specific privacy policy to ensure that civil liberties are safeguarded. To date, 30 centers have filed privacy policies with DHS.
.....

- Assisted fusion centers in developing privacy policies by producing a privacy policy development template; by providing training on its proper use; by conducting policy reviews; and by providing ongoing technical assistance to fusion centers on privacy policy documents;
- Worked with the PM-ISE, DHS, and DOJ to support the ISE-SAR EE; and

2 GOAL

- Met with representatives of privacy and civil liberties advocacy groups to listen to their concerns and incorporate them into revised ISE documents, such as the ISE-SAR Functional Standard.

Plans

As of the spring of 2009, the DHS, the FBI, and the DNI have completed ISE Privacy Protection Policies. The PGC has developed an action plan to help other participating agencies complete their own policies and to advise them as they move into Stage II of the implementation process.

In addition, the PGC will:

- Continue to provide technical assistance and training to fusion centers to ensure that they develop and implement privacy policies that are at least as comprehensive as the ISE Privacy Guidelines; and
- Develop an action plan for ensuring that private sector entities participating in the ISE adopt privacy protection policies that are at least as comprehensive as those outlined in the ISE Privacy Guidelines.

3 GOAL

GOAL 3: IMPROVE SHARING PRACTICES WITH FEDERAL, STATE, LOCAL, TRIBAL, AND FOREIGN PARTNERS

Enhance information sharing by standardizing practices, improving interagency coordination, developing guidance, and enabling infrastructure to support the information sharing mission.

3.1 The Nationwide SAR Initiative

Background

The Nationwide SAR Initiative builds on what law enforcement and other agencies have been doing for years—gathering information regarding behaviors and incidents associated with criminal activity—and establishes a process whereby SAR information can be shared among agencies to help detect and prevent terrorism-related criminal activity.

The NSI developed as a response to the mandate issued by the National Strategy for Information Sharing (NSIS) to establish a “unified process for reporting, tracking, and accessing [SARs].”³² The NSI process, as shown in Figure 6, involves a cycle of 12 steps that responds to the requirements articulated in the NSIS. The intended outcome is for Federal and SLT law enforcement organizations to standardize the way they gather, document, process, analyze, and share information about suspicious activity, while adequately protecting privacy and civil liberties according to law and regulation.

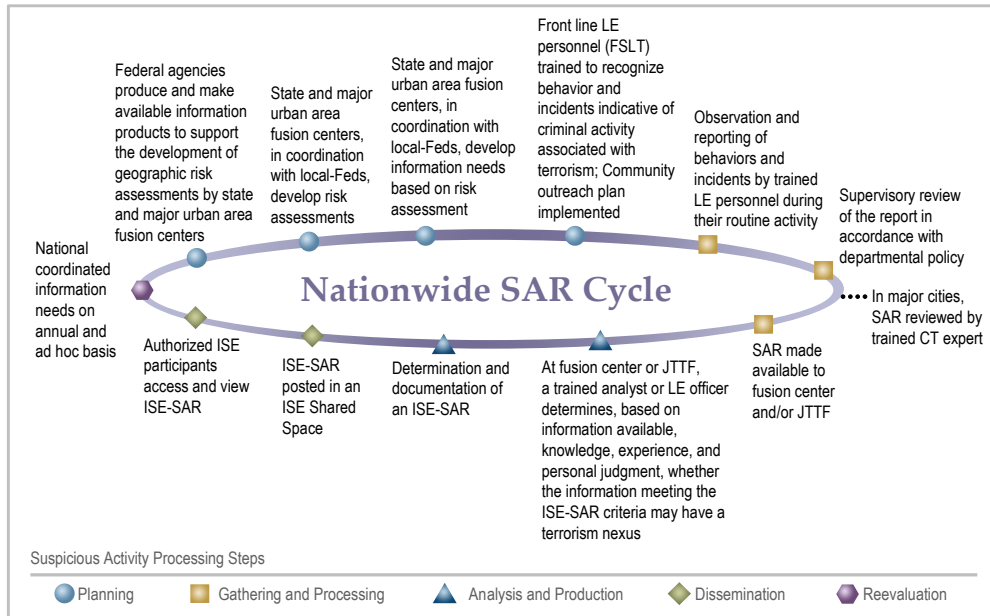


Figure 6. Overview of Nationwide SAR Cycle

The gathering, analysis, and sharing of SARs cannot take place in a vacuum. NSI participants need access to all-source information on terrorist threats and they must be trained to identify the behaviors and contexts that cause activities to be considered “suspicious.” There must

³² National Strategy for Information Sharing (NSIS) (October 2007), p. A1-6, 7.

3 GOAL

also be a mechanism for participants at all levels of government to be able to identify and share their information needs. For these reasons, the NSI cycle begins with a planning phase that is driven by the production and dissemination of information products about terrorist plans, intentions, and capabilities. These information products are then made available to ISE participants.

Threat assessments—largely, but not exclusively, produced by Federal agencies—may be derived from multiple information sources, may take varying forms, and may be issued as classified or unclassified reports. They contribute directly to local or regional risk assessments performed by State and major urban area fusion centers in collaboration with local DHS and FBI representatives.

Progress

Highlights of NSI activities during 2008-09 include:

- Publication of an NSI *Concept of Operations* (CONOPS) that provides a common understanding of the NSI process; defines the requirements that drive the process and its implementation; and describes the roles, missions, and responsibilities of NSI participating agencies.³³
- Completion of an *ISE-SAR Evaluation Environment Segment Architecture* that establishes short-term and long-term operational outcomes for the ISE-SAR EE;
- Development of an *ISE-SAR Evaluation Environment Implementation Guide* that identifies the methods for achieving the operational outcomes defined in the *Segment Architecture* in the context of the EE;
- Expansion of the EE to include 12 SLT participants and the DHS;
- Integration of the FBI eGuardian system into the NSI to ensure that all SAR information in eGuardian will be accessible through ISE Shared Spaces and vice versa;
- Completion of a CONOPS for incorporating information needs identified by fusion centers through local or regional risk assessments into the National Intelligence Priorities Counterterrorism Information Needs Framework;
- Completion of an ISE-SAR Privacy Analysis that clarified privacy requirements for the ISE-SAR EE and helped participants put in place privacy policies consistent with the requirements set forth in the ISE Privacy Guidelines;³⁴

.....
SAR TRAINING

In the last year, more than 10,000 officers and analysts have been trained in the fundamentals of the NSI process with a special emphasis on protecting privacy and civil liberties

- Release of Version 1.5 of the ISE-SAR Functional Standard, including improved selection criteria based on direct inputs from civil liberties advocacy organizations;
- Implementation of a governance process that provides a forum for stakeholder organizations and EE sites to address strategic NSI issues; and



³³ The NSI CONOPS and other baseline NSI documents are available on <http://www.ise.gov/pages/sar-initiative.html>.

³⁴ ISE Implementation Plan (November 2006), pp. 89-91.

- Development of a comprehensive program that trains agency executives, analysts, and front-line officers in the fundamentals of the NSI process, with a special emphasis on protecting privacy and civil liberties.

While the primary emphasis has been on establishing a uniform process, the NSI has also achieved some important operational results, as shown in the following examples:

- In March 2008, the Los Angeles Police Department (LAPD) established a departmental SAR process. This process, which is focused primarily on counterterrorism, has served as a precursor for the NSI. Since then, the LAPD has gathered and processed almost 1500 individual SARs, 51 of which were considered critical enough to forward directly to a Joint Terrorism Task Force (JTTF), and 21 of which contributed to investigations and arrests. In addition, the LAPD has made use of SARs in analyzing overall patterns and trends to support intelligence-led policing strategies.
- The eGuardian user base has surpassed 1,000 accounts, drawing participants from all parts of the country. In one four-month period, 346 incidents were reported to eGuardian, of which 280 fell into the category of suspicious activity. Of these, 15 were determined to have a potential terrorism nexus while 107 were resolved as having no connection to terrorism.
- An ISE-SAR EE site was established ahead of schedule at the Washington, D.C. MPD to support activities surrounding the Presidential Inauguration. From late December through Inauguration Day, MPD processed 88 SARs, 16 of which were forwarded to eGuardian as potentially terrorist-related.
- The DoD has identified a number of success stories from its use of eGuardian as part of the ISE-SAR EE. One incident, which involved stolen U.S. Marine uniforms, was initially reported to a local police department and then submitted to eGuardian by a fusion center.
- The Nuclear Regulatory Commission (NRC) cited one instance in which, through the use of eGuardian, its analysts detected a potential threat to one of its licensees that had not been reported in NRC's own SAR database.
- The Department of Transportation (DOT) has plans underway to stand up its first SAR database. The initiative has been approved by the DOT CIO Council, funding has been authorized, and the goal is to have the database up and running before the end of 2009. DOT analysts will review information in the database, perform patterns and trends analyses, and share information with other ISE agencies.

Plans

The results of the EE will drive most of the work on the NSI in FY 2010, to include:

- A comprehensive analysis and assessment of the EE implementation that summarizes performance measurement data, identifies lessons learned, and highlights best practices;
- Publication of a final version of the *Privacy and Civil Liberties Analysis* that provides clear guidance to any organization establishing a SAR process as part of the NSI;
- Publication of Version 2 of the *ISE-SAR Functional Standard*, incorporating lessons learned from the EE (scheduled for the spring of 2010); and

3 GOAL

- An implementation plan for a broader nationwide rollout of the NSI among Federal, State, local, and tribal law enforcement agencies across the country as well as with organizations in other communities where appropriate. This plan—to be developed by the end of calendar year 2009—will address program management issues and strategies for scaling the EE effort to accommodate a significantly broader set of participating agencies.

3.2 State and Major Urban Area Fusion Centers

Background

The ability to analyze and quickly draw appropriate inferences from multiple and sometimes disparate information sources lies at the heart of the challenge the ISE was established to address—to provide the right information to the right people in time to prevent terrorist attacks and to protect our communities and institutions.

Prior to 9/11, the information flow between Federal and SLT partners was not sufficiently robust to achieve a strong, effective, and productive nationwide information sharing partnership. Today, thanks to ISE efforts, that is changing. All 50 states have designated a primary fusion center to act as the focal point for the exchange of information between Federal agencies and SLT partners. Additionally, many urban areas have recognized the value of stronger local or regional partnerships, and have created their own fusion centers, bringing to 72 the number of designated centers nationwide. In addition, Federal agencies have made significant improvement in coordinating the planning and provision of grant funds, personnel resources, and technical assistance for these designated fusion centers.

The concept of information fusion is not new; it builds upon the intelligence-led policing concept that has been applied with great success for some time by law enforcement agencies across the country.

Figure 7 depicts the fusion process as a continuous cycle in which inputs from various sources—be they SLT or Federal—are brought together to create a holistic picture of the threats and vulnerabilities our communities are confronted with.³⁵ This information can then be used to reallocate resources, pursue investigations, or change the protective posture around critical infrastructure. Using this process, those charged with protecting our communities are better informed, and our people and institutions will be better protected.

Progress

- A collaborative effort led by the DHS and DOJ (Global Justice), with participation from other Federal and SLT agencies, resulted in publication of the *Baseline Capabilities for State and Major Urban Area Fusion Centers*.
- The PM-ISE and DHS jointly conducted a preliminary assessment of all fusion centers to broadly determine progress against the baseline capabilities, and to obtain, for the first time, insight into the rough order of magnitude of funds being expended by State and local governments in support of fusion center operations. The results of this first-order assessment were briefed to key stakeholders during the National Fusion Center Conference.

³⁵ Figure 7 represents a generalized view of a multi-source information handling process. The NSI cycle illustrated in Figure 6 is one representative instance that covers a single important information type—suspicious activity reports.

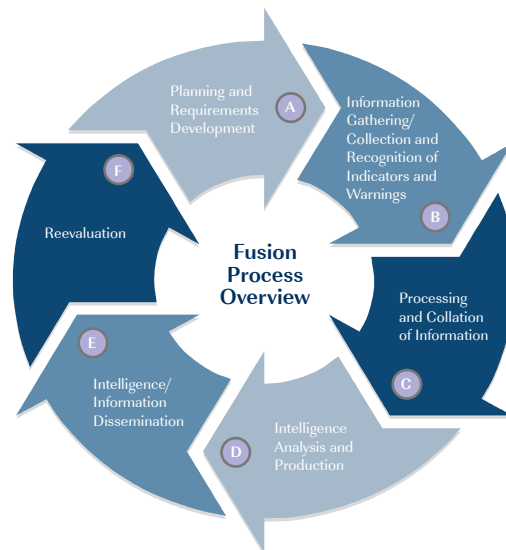


Figure 7. Overview of Fusion Process

- The National Fusion Center Coordination Group (NFCCG) led and coordinated efforts to improve the Federal Government’s support to a national, integrated network of fusion centers operating at a defined baseline level of capability. Specific achievements included:
 - Conducting regional and national conferences to address issues of broad concern to fusion centers;
 - Agreement by fusion center directors on key priority areas in which to focus their activities in the coming year, to include privacy and civil liberties;
 - Establishment of a national advisory body to advocate for the continued support of the fusion center mission across all levels of government; and
 - Publication of a communications strategy designed to assist fusion centers in gaining a stronger voice in the national security community.
- Federal agencies continued to deploy personnel in direct support of fusion center operations. DHS has deployed 36 Intelligence Operations Specialists to centers across the country, and intends to have deployed an officer to each of the 72 designated centers, as well as 10 Regional Directors, by the end of FY 2010.
- The Federal Emergency Management Agency revised the State Homeland Security Grant Program guidance to tie the use of DHS grant funds to fusion center progress in achieving the baseline capabilities.

Plans

In 2009-10, ISE activities to improve fusion center performance will focus on the following:

- Developing a consistent, replicable process for assessing centers against the *Baseline Capabilities*;

3
GOAL

- Evaluating fusion center funding expenditures to inform the debate over the appropriate level of Federal funding and to form the basis for the development of a sustainment strategy;
- Designing a set of outcome-based performance measures to demonstrate the value of a national integrated network of fusion centers operating in accordance with the baseline capabilities;
- Implementing a program to improve coordination of Federal support to fusion centers, to include options for an interagency program office; and
- Ensuring Federal support for the national network to address the following key priority areas: analysis and dissemination; alerts, warnings, and notifications; and privacy and civil liberties.

3.3 Improved Production and Dissemination

Background

Time-sensitive and strategic information products convey information critical to the CT and HS missions. This includes information on potential threats, terrorist intentions and techniques, and indications of planned future terrorist activities. Specific examples of products disseminated in the ISE include:

- *Alerts, Warnings, and Notifications (AWN)* and updates of time-sensitive information related to terrorist threats to our people, facilities, and institutions;
- *Situational Awareness Reporting* regarding significant events or activities occurring at the international, national, State, or local level; and
- *Strategic and Foundational Assessments* of terrorist threats to the United States.

At the Federal level, the Interagency Threat Assessment and Coordination Group (ITACG), a component of the NCTC, informs and helps shape national Intelligence Community (IC) products by providing advice, counsel, and subject matter expertise to better meet the needs of SLT organizations. Staffed with personnel from Federal and SLT agencies, the ITACG identifies, reviews, and assesses relevant material of interest to SLT entities.³⁶ It also supports the appropriate dissemination of federally-coordinated terrorism-related information products through existing websites and distribution channels of DOJ, DHS, and other agencies.

At the SLT level, fusion centers are the critical nodes in the production and dissemination processes. These centers rely on their own analytic capabilities, as well as those of Federal agencies, to ensure that SLT governments are aware of terrorist threats and indicators. The FBI and the DHS are accelerating the deployment of both classified and unclassified Federal information systems to fusion centers, to better facilitate the necessary sharing of critical information.

The Law Enforcement Information Sharing Service (LEISS)—a PM-ISE endorsed and sponsored effort—has directly contributed to improving the quality and quantity of information available at fusion centers. LEISS is an initiative of DHS’s Immigration and Customs Enforcement (ICE), in collaboration with DOJ, to leverage existing tools and capabilities to expand bi-directional sharing with other Federal and SLT partners. This effort formalizes and standardizes previously

³⁶ Although part of the NCTC, the ITACG Director is a DHS employee and the Deputy Director comes from the FBI.

ad hoc policies and processes for sharing of law enforcement information, providing for the broader collaboration on investigations.

Progress

Highlights of production and dissemination activities during 2008-09 include:

- Development, by the ITACG, working with DHS and FBI, of an SBU product called the “Roll Call Release”. This product is written specifically for SLT first responders, and provides information on terrorist tactics, techniques, terrorism trends; and indicators of suspicious activity. These one-page reports are written on an ad-hoc basis and deal with a single topic.
- Publication of joint DHS/FBI secure space standards to facilitate deployment of classified networks into fusion centers. (Previously, fusion centers wishing to construct a secure room to house classified computer terminals had to apply different standards for DHS and FBI networks.)
- Deployment of the FBI Secret domain network (FBINet) to 33 fusion centers, with access granted to 151 SLT permanently assigned SLT personnel. In addition, DHS installed Homeland Security Data Network (HSDN) terminals at 29 fusion centers and created accounts for 363 SLT personnel.
- NCTC improved the value of its Secret level online repository (NOL S) to SLT customers by:
 - Working with the Central Intelligence Agency (CIA) and other IC agencies to increase the number of products posted to NOL-S;
 - Conducting an awareness campaign, in conjunction with the DHS, to inform SLT organizations about NOL-S and its potential value to their CT and HS missions;

.....
LEISS

There are plans to expand the LEISS capability to include Texas and New Mexico. Along with the already existing ties with Arizona, this will allow LEISS to support DHS’s high-priority Southwest border initiative, designed to crack down on Mexican drug cartels through enhanced border security.

.....

- Developing a new product line called Terrorism Information Sharing Products (TIPS). TIPS are generated from more highly classified products and are downgraded because of their relevance to fusion centers; and
- Launching a new daily product called the “Terrorism Summary,” a Secret-level digest of terrorism-related intelligence of interest to Federal and non-Federal law enforcement, security, and military personnel.
- The PM-ISE performed a business process analysis of AWN information flows and data elements. This analysis—coordinated among PM-ISE, the DHS, the FBI, ITACG, and the NCTC—was included in Version 2 of the ISE EAF.

3
GOALS**Plans**

In 2009-10, ISE activities to improve intelligence production and dissemination will focus on the following:

- Improving the ITACG so it will be a better advocate for SLT needs. With a broader and deeper understanding of national intelligence products and SLT intelligence needs, ITACG will do a better job of enabling the production of SLT-specific products. This in turn will help SLT analysts provide better guidance regarding SARs to law enforcement, to develop more thorough risk assessments, and to better identify local information needs. The ITACG can then better advocate for these needs through the national CT information needs process, managed by NCTC.
- Improving dissemination of AWN. The PM-ISE has begun to work with other agencies to address significant gaps in the national AWN process that impede the effective reporting, notification, and tracking of information related to time-sensitive terrorist threats to our people, facilities, and institutions. Recommended solutions will be coordinated and implemented with relevant Federal agencies, SLT governments, and the private sector.
- Completing deployment of classified networks to all fusion centers. With the publication of the joint DHS/FBI secure space standard, fusion centers can now construct secure spaces that are accredited to house either FBINet or HSDN terminals. This will reduce deployment time and ensure that a greater number of fusion centers are able to take advantage of expanded access to these classified networks.

3.4 Sharing with Foreign Partners

Background

Recommendations in the response to Presidential Information Sharing Guideline 4 and the NSIS recognize that the “effective and substantial cooperation with our foreign partners requires sustained liaison efforts, timeliness, flexibility, and the mutually beneficial exchange of many forms of terrorism-related information.” The ISE fosters this kind of cooperation by providing a community of interest within which agencies can collaborate on the bi-directional sharing of information with foreign partners. This includes the identifying best practices for negotiating foreign sharing agreements and the development of standards for safeguarding and handling foreign government information.

Progress

A highlight of our 2008-09 activities regarding the sharing of information with foreign partners was the consolidation and sharing of more than 400 unclassified agreements or agreement descriptions between Federal agencies and their foreign partners via the ODNI’s Foreign Intelligence Relationship Enterprise (FIRES) system. This new tool assists officials involved in negotiating agreements and arrangements with foreign governments. The unclassified agreement and arrangement information provides FIRES users with insight into existing relationships between the U.S. and its foreign partners. (This information is also available through HSDN.)

Plans

Planned activities regarding information sharing with foreign partners during 2009-10 include the following:

3
GOAL

- Ensuring that ISE Federal agencies responsible for working with foreign partners have established internal procedures to expedite disclosure decisions and have identified foreign disclosure officers to make such decisions;
- Continuing to encourage broad use of the *Checklist of Issues for Negotiating Terrorism Information Sharing Agreements and Arrangements* by contacting those Federal agencies who make such agreements but have not yet identified themselves as users of the Checklist;
- Enhancing the Repository of Foreign Sharing Agreements by broadening access to the repository and including either more agreements with foreign partners or metadata about such agreements; and
- Surveying ISE Federal agencies to identify information sharing best practices or impediments among our foreign partners.

4 GOAL

GOAL 4: INSTITUTIONALIZE SHARING

Make information sharing routine through championing, leading, using, and sustaining efforts to standardize policies, resources, business practices, and technologies.

4.1 ISE Architecture Program

Background

A smoothly functioning ISE requires IT systems and infrastructures that support the development, integration, and sustained operation of standardized information sharing systems by all participants. The ISE Architecture program meets this goal by aligning and connecting the diverse myriad of IT systems and infrastructures used by ISE participants—which are often isolated by their very different and sometimes conflicting policies, business practices, and cultures—into a more uniform, seamless, well-defined set of interconnected systems. Figure 8 shows how the ISE architecture program fits into the Federal Enterprise Architecture (FEA), serving as a bridge between individual component architectures.

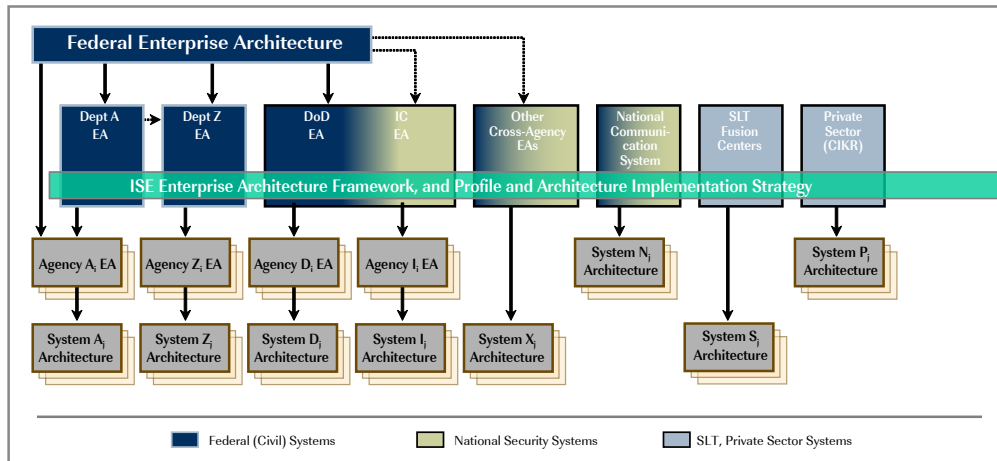


Figure 8. ISE Architecture Program Bridging ISE Community Enterprise Architectures

Progress

Highlights of ISE Architecture efforts in 2008-09 include:

- Version 2 of the *ISE Enterprise Architecture Framework* provides technology and architecture guidance to assist ISE participants in adapting enterprise architectures, especially Information Sharing Segment Architectures, to interoperate within the ISE. It provides greater definition of SAR, Identification and Screening, and AWN business processes, delineates the roles and responsibilities of ISE Implementation Agents, and includes guidance for implementing information sharing services in the ISE. OMB’s *Federal Segment Architecture Methodology* incorporated the concepts from the ISE EAF as a best practice.

- Version 2 of the *ISE Profile and Architecture Implementation Strategy (PAIS)* outlines the criteria for building and operating ISE Shared Spaces. It also provides expanded implementation guidance for developers of segment architectures and their associated operational components.

.....
APPLYING THE ISE EAF TO OTHER DOMAINS

Other government-wide information sharing initiatives—including the Next Generation Aviation Transportation System, the Maritime Domain Awareness Initiative, and the Federal Health Information Sharing Environment—are leveraging concepts, principles, services, and standards from the ISE Architecture program, continuing the move towards a unified, government-wide approach to IT architecture and standards for information sharing.

.....

- ISE requirements were incorporated into the *Federal Transition Framework Catalog*, OMB’s cross-agency investment guidance. This guidance can be used to help identify and monitor Federal agency investment planning compliance with ISE business and technology requirements.
- The PM-ISE is working closely with the Federal CIO Council to support its Identity, Credential, and Access Management (ICAM) Roadmap initiative, as well as with the National Science and Technology Council Subcommittee on Biometrics and Identity Management, as part of the government-wide effort to implement a common identity and access management solution supporting all ISE participating organizations.

Plans

In 2010, the ISE Architecture program plans to:

- Issue *ISE EAF, Version 3*, which will provide more detailed guidance on ISE Implementation Agents, as well as more detailed about required information-flows for SAR, Identification and Screening (Terrorist Watchlist components, cargo, and people screening), and the AWN business processes;
- Issue *ISE PAIS, Version 3*. This will provide more technical specificity on interfaces between ISE Shared Spaces and interconnecting infrastructures provided by ISE Implementation Agents, including enhanced interoperability and interconnectivity between CUI/SBU networks and systems;
- Develop a *CUI/SBU Interconnectivity Concept of Operations and Segment Architecture* to define requirements and to reconcile interoperability issues between CUI/SBU networks, portals, and systems; and
- Develop a systems architecture reference guide for fusion centers that provides guidance on designing and operating information systems in accordance with the *Baseline Capabilities for State and Major Urban Area Fusion Centers*.

4
GOALS

4.2 Common Terrorism Information Sharing Standards Program

Background

The need for common ISE standards is cited both in IRTPA and the NSIS—an explicit recognition that common standards are fundamental building blocks of effective and efficient information sharing.³⁷ Responding to that need, the Common Terrorism Information Sharing Standards (CTISS) program develops business process-driven, performance-based standards that support preparing terrorism-related information for maximum distribution and access.

- *Functional Standards* set forth rules, conditions, guidelines, and characteristics of data and mission products supporting ISE business processes; and
- *Technical Standards* document methodologies and practices to design and implement information sharing technology capability into ISE systems to enable interoperability and interconnectivity across the ISE.

In January 2008, the PM-ISE issued the first CTISS Functional Standard (ISE-FS-200) providing a business process and data structural foundation for sharing ISE SARs.³⁸ This standard also supports the protection of privacy and civil liberties by designating a number of data elements as “privacy fields,” i.e., fields containing personal information that require and receive special protection. ISE Shared Spaces provide the IT solutions for ISE participants to store and share this standardized information while still maintaining local oversight and control.

Progress


Highlights of CTISS efforts in 2008-09 included:

- Issuance of new Technical Standards for Information Assurance, Core Transport, and Identity and Access Management in the ISE.³⁹
- Release of the updated ISE-SAR Functional Standard (Version 1.5), which strengthens ISE-SAR privacy controls and refines terrorism identification criteria to better safeguard First Amendment rights. Developed in partnership with national privacy and civil liberties advocates, this update provides clearer implementation guidance and incorporates stronger privacy protection into ISE-SAR data exchanges.

.....
**COMMENT ON THE
 ISE-SAR FUNCTIONAL STANDARD**

“The revised guidelines for suspicious activity reporting establish that a reasonable connection to terrorism or other criminal activity is required before law enforcement may collect Americans’ personal information and share it within the ISE. These changes to the standard, which include reiterating that race cannot be used as a factor to create suspicion, give law enforcement the authority it needs without sacrificing the rights of those it seeks to protect.”

Michael German, National Policy Council
 American Civil Liberties Union

 ³⁷ IRTPA (as amended) §016(f)(2)(A)(ii).
³⁸ See <http://www.ise.gov/pages/sar-initiative.html>.
³⁹ ISE-G-106, ISE-G-107, and ISE-G-109. See <http://www.ise.gov/pages/ctiss.html>.

- Determining that an updated Terrorist Watchlist Person Data Exchange Standard (TWPDES, Version 1.2b) was unclassified and could be made available for broader release to Federal, State, local, and tribal partners.

4
GOAL**Plans**

Plans for CTISS in 2010 include:

- Updating the technical standards for Information Assurance and Identity and Access Management. This update will incorporate new information assurance and IT security guidance and standards from Federal Government initiatives, such as the Comprehensive National Cyber Security Initiative; will provide increased specificity on ISE participant and ISE Implementation Agent responsibilities; and will identify specific role-based access criteria.
- Issuing ISE Functional Standard-Suspicious Activity Reporting, Version 2.0. Version 2.0 will incorporate the findings and recommendations from the ISE-SAR EE and will reflect updated ISE-SAR business processes and rules, along with linkages to other communities participating in the NSI.
- Examination of options for developing additional CTISS Functional Standards.

PART THREE – MANAGING THE ISE: 2009 AND BEYOND

“I would seek an OMB Version 2.0, where those two arms of the agency [management and budget] are better integrated and you see a more unified whole between performance and budgeting.”

— Peter R. Orszag, Director of the Office of Management and the Budget

THE INFORMATION SHARING ENVIRONMENT FRAMEWORK

Overview

Over the past three years, the ISE Implementation Plan has provided the key programmatic direction for managing the actions of the ISE. Based on our past accomplishments, the PM-ISE developed the Performance and Investment Integration Program to continue our goal-focused progress and move the ISE to new levels of maturity.

The ISE Performance and Investment Integration Program builds on previous efforts to establish ISE-wide processes for managing performance and investments and to allocate appropriate resources towards ISE goals. The Performance and Investment Integration Program consists of four main components (see Figure 9):

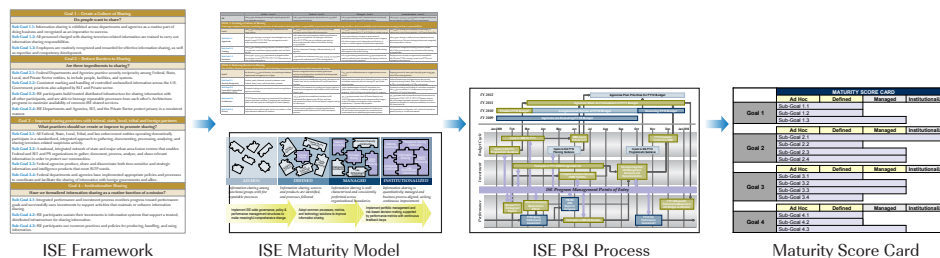


Figure 9. Components of the ISE Performance and Investment Integration Program

1. **ISE Framework:** Creates linkages between goals and sub-Goals down to the level of critical activities and measures for moving the ISE to an *institutionalized* state.
2. **ISE Maturity Model:** Defines levels of maturity for ISE goals and sub-goals from an *ad hoc* to an *institutionalized* state.
3. **ISE Performance and Investment (P&I) Process:** Links performance measures, investment decisions, and project management activities to the Federal Government budgeting process.
4. **ISE Maturity Score Card:** Provides an ISE implementation summary to convey progress towards the ISE goals.

The remainder of this section describes each of these components in more detail.

The ISE Framework

To better define and manage ISE implementation, the PM-ISE developed and adopted the new ISE Framework (“the Framework”). The Framework creates critical linkages between four primary and enduring ISE goals, fourteen sub-goals, and a resulting set of outcomes, objectives, products, activities, and associated performance measures.

Table 1 shows the alignment of the Framework’s goals and sub-goals. (Appendix A also includes additional information on outcomes and objectives.)

Table 1. ISE Goals and Sub-Goals

| |
|---|
| Goal 1 – Create a Culture of Sharing |
| Do people want to share? |
| <p>Sub-Goal 1.1: Information sharing is exhibited across departments and agencies as a routine part of doing business and recognized as an imperative to success.</p> <p>Sub-Goal 1.2: All personnel charged with sharing terrorism related information are trained to carry out information sharing responsibilities.</p> <p>Sub-Goal 1.3: Employees are routinely recognized and rewarded for effective information sharing, as well as expertise and competency development.</p> |
| Goal 2 – Reduce Barriers to Sharing |
| Are there impediments to sharing? |
| <p>Sub-Goal 2.1: Federal Departments and Agencies practice security reciprocity among Federal, State, Local, and Private Sector entities, to include people, facilities, and systems.</p> <p>Sub-Goal 2.2: Consistent marking and handling of controlled unclassified information across the U.S. Government; practices also adopted by SLT and Private sector.</p> <p>Sub-Goal 2.3: ISE participants build trusted distributed infrastructure for sharing information with all other participants, and are able to leverage repeatable processes from each other’s Architecture programs to maximize availability of common ISE shared services.</p> <p>Sub-Goal 2.4: ISE Departments and Agencies, SLT, and the Private Sector protect privacy in a consistent manner.</p> |
| Goal 3 – Improve sharing practices with federal, state, local, tribal and foreign partners |
| What practices should we create or improve to promote sharing? |
| <p>Sub-Goal 3.1: All Federal, State, Local, Tribal, and law enforcement entities operating domestically participate in a standardized, integrated approach to gathering, documenting, processing, analyzing, and sharing terrorism-related suspicious activity.</p> <p>Sub-Goal 3.2: A national, integrated network of state and major urban area fusion centers that enables Federal and SLT and PS organizations to gather, document, process, analyze, and share relevant information in order to protect our communities.</p> <p>Sub-Goal 3.3: Federal agencies produce, share and disseminate both time-sensitive and strategic information and intelligence products that meet SLTP needs.</p> <p>Sub-Goal 3.4: Federal departments and agencies have implemented appropriate policies and processes to coordinate and facilitate the sharing of information with foreign governments and allies.</p> |
| Goal 4 – Institutionalize Sharing |
| Have we formalized information sharing as a routine function of a mission? |
| <p>Sub-Goal 4.1: Integrated performance and investment process monitors progress toward performance goals and successfully uses investments to support activities that maintain or enhance information sharing.</p> <p>Sub-Goal 4.2: ISE participants sustain their investments in information systems that support a trusted, distributed infrastructure for sharing information.</p> <p>Sub-Goal 4.3: ISE participants use common practices and policies for producing, handling, and using information.</p> |

Consistent with the vision, strategic goals, and fundamental concepts embodied in the ISE Implementation Plan and the NSIS, the Framework represents a new approach to managing the ISE that ties individual products and activities directly to specific objectives, outcomes, goals, and sub-goals. It provides a common understanding of the problems to be solved, the essential capabilities that constitute the ISE, and the actions needed to ensure that these capabilities are developed and deployed in a manner “consistent with national security and with applicable legal standards relating to privacy and civil liberties.”⁴⁰

The Framework serves as a tool for managing ISE activities and assessing progress against our primary four goals. Figure 10 shows how the Framework can be used to drive specific outcomes, objectives, products, activities, and performance measures.

Goal 1: Create a Culture of Sharing – Establish employee behaviors including awareness of information sharing policies, responsibility to perform information sharing activities, and accountability and incentives for carrying out those responsibilities. Do people want to share?

Sub-Goal 1.1: Information sharing is exhibited across departments and agencies as a routine part of doing business and recognized as an imperative to success.

| Outcome | Objective | Product | Activities | Spring '09 Measures | Resource Requirements |
|---|--|---|--|---|-----------------------|
| 1.1.1: Employees are evaluated for information sharing expertise and competency development. | 1.1.1.1: Develop guidance to help ISE agencies develop information sharing performance elements for inclusion in applicable employee performance appraisals. | ISE Guidance 105 – Inclusion of Information Sharing Performance Evaluation Element in Employee Performance Appraisals | Follow-up with agencies on implementation. | % of ISE agencies have distributed (or intend to distribute) guidance for incorporating information sharing elements into performance appraisals. | |

Figure 10. Example of Linkage of Goals to Performance Measures

Linking the ISE Maturity Model to the ISE Framework

The PM-ISE developed an ISE Maturity Model (Figure 11) to periodically assess ISE progress at the sub-goal level. On a regular basis, the PM-ISE and stakeholders will use this model to assess progress, allowing them to determine how far the ISE has come in its efforts; to identify the steps necessary to reach an *institutionalized* state; and to help drive future ISE performance management and investment activities.

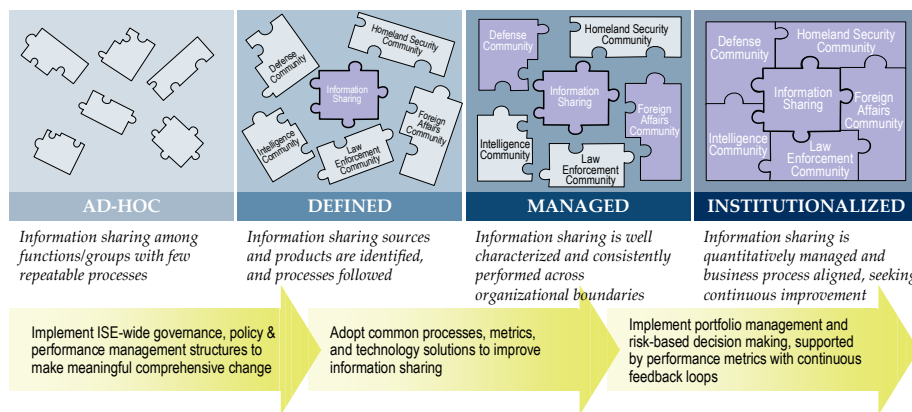


Figure 11. ISE Maturity Model Concept

40 IRTPA (as amended), §1016(b)(1)(A).

Table 2 shows the linkage of the ISE Maturity Model to the ISE Framework at the sub-goal level. Each sub-goal describes the conditions and behaviors to be expected in the ISE at each state of maturity, and serves as a “yardstick” for gauging progress toward our goals. The PM-ISE will assess the relative maturity against the criteria of each stage of development and aggregate this information at the sub-goal, goal, and overall ISE level to paint a clearer picture of how far the ISE has come and where future attention is needed. The PM-ISE will report on progress in updates to partner agencies as well as to OMB, Congress, and other stakeholders.

Table 2. Maturity Model – Definitions for each State of Maturity for Goals and Sub-Goals

| | Ad Hoc – Level 1 | Defined – Level 2 | Managed – Level 3 | Institutionalized – Level 4 |
|---|---|---|--|---|
| ISE | Information sharing occurs among functional groups with few repeatable processes | Information sharing sources and products are identified and processes followed | Information sharing is well characterized and consistently performed across organizational boundaries | Information sharing is quantitatively managed and business process aligned, seeking continuous improvement |
| GOAL 1: Create a Culture of Sharing | | | | |
| Encourage employee behaviors including awareness of information sharing policies, responsibility to perform information sharing activities, and accountability and incentives for carrying out those responsibilities | | | | |
| Goal 1 | Information sharing occurs through individual acts and heroic efforts | Information sharing occurs as a job function, though resistance and misinformation are common | Information sharing is recognized as a part of the job and is valued and measured for its contribution to mission success | Information sharing occurs between communities, is natural and a lack of sharing leads to swift corrective action |
| Sub-Goal 1.1 Appraisals | Information sharing is sometimes acknowledged but is not explicit in performance objectives and appraisals and is never a priority requirement | Information sharing is frequently added to performance objectives and appraisals of employees with direct ISE responsibilities, but not uniformly, and rarely to other employees with indirect information sharing responsibilities | Information sharing is routinely a requirement in performance objectives of all employees as part of agency ISE mission support and is frequently mentioned as a criteria in a broad segment of performance appraisals | Information sharing is exhibited across departments and agencies as a routine part of doing business and recognized as an imperative to success |
| Sub-Goal 1.2 Training | Information sharing training may exist, but when it does, it is occasional, inconsistent, agency-specific, and not tied to the ISE | ISE Core Awareness Training is offered uniformly in all agencies | Agencies develop and implement mission-specific training that supports information sharing | All personnel charged with sharing terrorism related information are trained to carry out information sharing responsibilities |
| Sub-Goal 1.3 Incentives | Information sharing incentive awards or programs either do not exist, or are folded into other incentives without an information sharing focus | Initial efforts are underway to provide awards and incentive programs for individual information sharing efforts | Information sharing awards and recognition programs are explicitly defined, reach throughout the agency, and focus on cross-community behaviors | Employees are routinely recognized and rewarded for effective information sharing, as well as expertise and competency development |
| GOAL 2: Reduce Barriers to Sharing | | | | |
| Use of Policy, business process and practices, and technology to remove obstacles and enable information sharing | | | | |
| Goal 2 | No formal recognition of barriers, no coordination between departments and agencies to mitigate | Barriers recognized and documented; governance structures and approaches are defined (including people, policies, and technologies) | Execution of a defined process to mitigate barriers across the ISE | Ongoing process for proactively identifying and mitigating information sharing barriers |
| Sub-Goal 2.1 Security Reciprocity | Limited, mostly bilateral, reciprocity between some Federal, State, Local, and Private Sector partners | Specific policies are established and usually followed at the Federal level but do not extend to SLT and Private Sector Partners | Policies are harmonized at the Federal level and are written to facilitate reciprocity with and among SLT and Private Sector Partners | Federal Departments and Agencies practice security reciprocity among Federal, State, Local, and Private Sector entities, to include people, facilities, and systems |
| Sub-Goal 2.2 Controlled Unclassified Information (CUI) | Disparate marking and control policies exist among Federal agencies and States | Common CUI framework for marking and control policies is established and approved with Federal and SLT and Private Sector input | Initial implementation of the CUI framework via a governance structure is underway, and agencies are designing, implementing, and coordinating CUI programs | Consistent marking and handling of controlled unclassified information across the U.S. Government; practices also adopted by SLT and Private sector |
| Sub-Goal 2.3 Architecture | ISE participants have begun to incorporate ISE Architecture program principles into their IT programs and architecture plans, and have a plan for building an ISE Shared Space(s) | ISE participants have established interfaces to ISE Implementation Agents in the ISE Core and have documented how their ISE Shared Space(s) support sharing of information | ISE participants sustain their ISE Shared Space(s) and supporting systems while clearly demonstrating linkages to the ISE Architecture program in their respective architectures, IT systems and portfolios | ISE participants build trusted distributed infrastructure for sharing information with all other participants, and are able to leverage repeatable processes from each other's Architecture programs to maximize availability of common ISE shared services |
| Sub-Goal 2.4 Privacy | Individual privacy policies exist, but are not uniform in their requirements to address ISE concerns | Uniform privacy guidelines and training materials are coordinated across Federal and SLT and Private Sector partners | Written and uniform privacy policies for Federal and SLT and Private Sector partners are coordinated and implemented via an established governance process | ISE Departments and Agencies, SLT, and the Private Sector protect privacy in a consistent manner |

Table 2. Maturity Model – Definitions for each State of Maturity for Goals and Sub-Goals (continued)

| | Ad Hoc – Level 1 | Defined – Level 2 | Managed – Level 3 | Institutionalized – Level 4 |
|--|---|---|---|---|
| ISE | Information sharing occurs among functional groups with few repeatable processes | Information sharing sources and products are identified and processes followed | Information sharing is well characterized and consistently performed across organizational boundaries | Information sharing is quantitatively managed and business process aligned, seeking continuous improvement |
| GOAL 3: Improve Sharing Practices with Federal, State, Local, Tribal, and Foreign Partners | | | | |
| Enhance information sharing by standardizing practices, improving interagency coordination, and developing guidance and enabling infrastructure to support the information sharing mission | | | | |
| Goal 3 | Limited information sharing occurs without common practices, often relying on personal relationships; inconsistent mechanisms to improve information sharing | Internal information sharing practices exist and are defined; leading practices are identified but not incorporated into improvement efforts | Information sharing processes are coordinated and operational within and between Federal, State, Local, Tribal, and Private partners; best practices and lessons learned from all ISE participants are used to improve information sharing | Information sharing occurs across all levels of government, the Private Sector, and foreign partners; ISE has a process to improve existing and implement new capabilities to support the information sharing mission |
| Sub-Goal 3.1 NSI | Value of suspicious activity reporting (SAR) is understood, but no nationwide standards, training, or coordination for sharing SAR exist | The planning of coordinated SAR information sharing is underway, based on an agreed upon nationwide standard | A consistent approach to sharing SARs has been adopted, and SAR processes have been implemented on a limited scale across all levels of government | All Federal, State, Local, Tribal, and law enforcement entities operating domestically participate in a standardized, integrated approach to gathering, documenting, processing, analyzing, and sharing terrorism-related suspicious activity |
| Sub-Goal 3.2 Fusion Centers | SLT agencies have limited, occasional, and uncoordinated access to Federal information and vice versa | Baseline Capabilities (BLC) for State and Major Urban Area Fusion Centers are published and high-level assessment processes are developed | In-depth, periodic BLC assessments are completed at designated Fusion Centers; assessments demonstrate a national network capable of effectively gathering, documenting, processing, analyzing, and sharing all crimes-all hazards information | A national, integrated network of State and major urban area fusion centers that enables Federal and SLT and PS organizations to gather, document, process, analyze, and share relevant information in order to protect our communities |
| Sub-Goal 3.3 ITACG (Fusion Centers) | State and local information needs are not being met by Federal products | Initial operating capability of ITACG established, including inter-departmental MOAs, establishment of processes and assignment of personnel | SLTP requirements are being incorporated into Federal information and intelligence products; Federal agencies have improved their ability to produce, share and disseminate both time-sensitive and strategic information and intelligence products that meet SLT needs | Federal agencies produce, share and disseminate both time-sensitive and strategic information and intelligence products that meet SLTP needs |
| Sub-Goal 3.4 Foreign Partners | Bilateral efforts between discrete Federal agencies and foreign governments | Federal government has some coordination in executing bilateral agreements with a common checklist of issues for negotiating information sharing agreements | Federal, SL governments have a coordinated approach to executing bilateral agreements with foreign partners to include common internal procedures to expedite disclosure decisions | Federal departments and agencies have implemented appropriate policies and processes to coordinate and facilitate the sharing of information with foreign governments and allies |
| GOAL 4: Institutionalize Sharing | | | | |
| Make information sharing routine through championing, leading, use, and sustainment of efforts to standardize policies, resources, business practices, and technologies | | | | |
| Goal 4 | Policies, resources, business practices, and technologies are inadequate or misaligned to address the information sharing mission | Information sharing capabilities are prioritized, documented, and adopted by ISE stakeholders | Information sharing initiatives are championed and coordinated across Federal, State, Local, Tribal, and Private partners | Information is efficiently and effectively shared across all levels of government and the private sector and continues to improve and evolve as needed |
| Sub-Goal 4.1 Performance and Investment Integration | Limited performance and investment data exists upon which to make information sharing planning and implementation decisions based on agency mission needs | Initial performance and investment metrics identified and data collected for a core prioritized set of information sharing programs; initial steps by some agencies taken to act on performance and investment data | Integrated performance and investment process supports the Federal planning and budgeting cycle and is used to make management decisions for information sharing programs nationwide | Integrated performance and investment process monitors progress toward performance goals and successfully uses investments to support activities that maintain or enhance information sharing |
| Sub-Goal 4.2 Enterprise Architecture/ Capital Planning and Investment Control (CPIC) Integration | ISE participants' respective enterprise architecture strategies include some cross-agency ISE Architecture program principles with initial linkages established to CPIC processes | ISE participants have incorporated ISE Architecture program principles and artifacts into their current and long-term planning and enterprise architectures, identifying opportunities for consolidation and reuse, to achieve long-term ISE investment strategies | ISE participants have fully integrated ISE Architecture program principles into their CPIC processes, and can demonstrate clear linkages between programs, IT systems and projects in their EA transition strategies; and IT investments in their investment portfolios | ISE participants sustain their investments in information systems that support a trusted, distributed infrastructure for sharing information |
| Sub-Goal 4.3 CTISS | ISE participants are beginning to define business processes, information flows, and data standards for information sharing | ISE participants have documented business processes, information flows, and data standards. A transition strategy has been developed consistent with CTISS Functional Standards. Relevant CTISS Technical Standards have been incorporated in future implementation efforts | ISE participants' daily practice involves the use of business processes, information flows, and data standards consistent with CTISS Functional Standards and implemented information sharing systems are consistent with CTISS Technical Standards. Formalized, repeatable policies are in place to govern the exchange and reuse of information | ISE participants use common practices and policies for producing, handling, and using information |

The Performance and Investment Integration Process

As shown in Figure 12, execution of the P&I program rests on three pillars: **Budget**, **Investment**, and **Performance**. To integrate information and use it in programmatic decision-making, data must be gathered and synthesized across all three pillars concurrently.

- **Budget:** The Budget pillar acts as the anchor for the overall process. Tied to the Federal Government budgeting process, this pillar identifies the primary touch points for influencing the budgeting process within Federal agencies and OMB.
- **Investment:** The Investment pillar focuses on the collection and assessment of resource data regarding ISE priorities. Using existing data collection tools and processes, the PM-ISE will minimize redundancies and duplication of effort in data collection. Program reviews will also be conducted to ensure that programs are meeting the intended results.
- **Performance:** The Performance pillar combines existing collection mechanisms to assess the progress toward maturity of ISE activities, their progress toward meeting the end goal of institutionalization, and the effective and efficient performance of information sharing across the ISE. To measure performance, the PM-ISE will examine the ISE across four stages of maturity: *Ad-Hoc*, *Defined*, *Managed*, and *Institutionalized*.

To execute the Performance and Investment Integrated Process (“the Process”), tasks will be completed in five major steps involving the definition of programs, the issuance of guidance, the development of data call requirements data, the analysis of data submissions, and the management of program decisions. These steps take place as part of a yearly cycle and are identified as “ISE Program Management Points of Entry” in Figure 12.

The Process must deal with four budget years simultaneously. This chart shows Planning, Programming, Budgeting, and Execution for 2009-12.

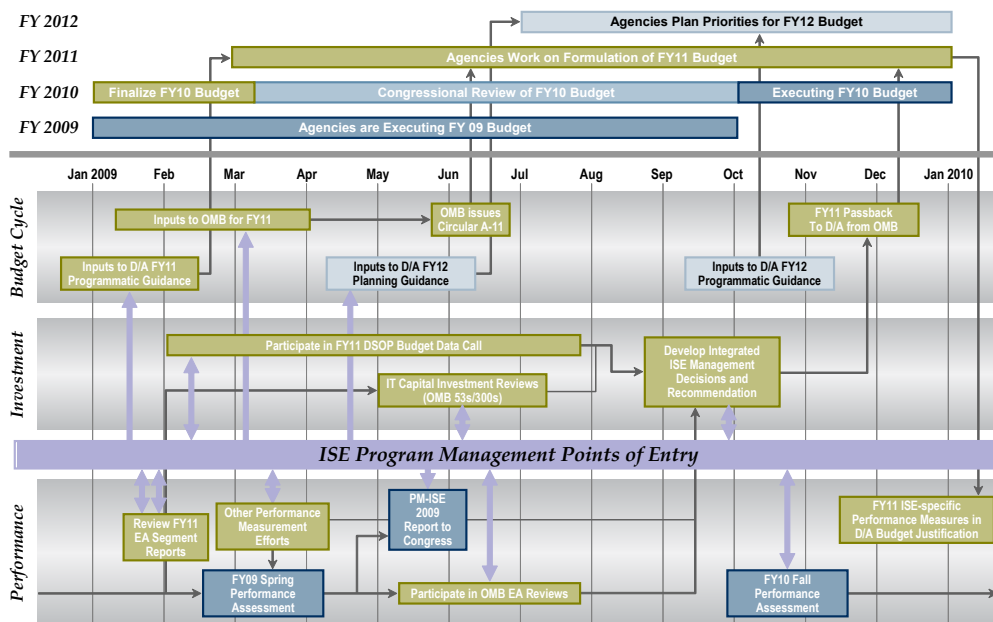


Figure 12. Performance and Investment Integration Activities and Timing

Step 1: Define Programs

The more completely programs are defined, the easier it is to identify the steps required to accomplish their goals and to develop accurate measures for gauging their progress. The ISE Framework provides definition for the ISE, creating a linkage of goals, sub-goals, outcomes, objectives, products, activities, and performance measures.

Step 2: Develop Guidance

Including ISE priorities in the annual budget guidance to Federal agencies will help ensure that ISE programs are properly considered in the budgeting process. The Process aims to affect the following guidance vehicles: Agency Planning Guidance, Agency Programmatic Guidance, OMB guidance, and OMB Passback Recommendations. By understanding the budget planning opportunities and the required timelines, program managers can determine how to best represent their programs' needs and to develop the specific language for each guidance document.

Step 3: Develop Data Call Requirements

Once ISE priorities are reflected in guidance, the type of information needed to manage the programs will be determined. The existing requirements will be reconciled, and new requirements will be identified for the collection of data. The best sources of information to satisfy these requirements include bi-annual performance assessments, the NCTC Directorate of Strategic Operational Planning data call, budget justifications, Enterprise Architecture Segment Reviews, Capital Planning and Investment Reviews, and individual program reviews. By collecting data at various points in the Process, a holistic picture of a program's progress and required resources will be presented.

Step 4: Analyze Data Submissions

The Process allows for the collection of data from appropriate sources and analysis of the information for use in the development of programmatic decisions.

Step 5: Program Decisions

Using the information collected from data calls, program managers will be better informed and more capable of determining exactly which programmatic decisions need to be made (e.g. process, policy, or resource decisions). Based on analysis of this information, recommendations will be provided to the PM-ISE and ISE stakeholders.

The Process will combine the assessments of progress and performance with the investment data to develop integrated management recommendations. This part of the process corresponds with the box in Figure 12 labeled "Develop Integrated ISE Management Decisions and Recommendations." This assessment could drive the direction of the programs and programmatic decisions reflected in the PM-ISE/OMB Passback recommendations, be reflected in ISE programmatic guidance for the following year, and be reported to Congress and other stakeholders.

The ISE Maturity Score Card

The ISE Maturity Score Card offers a means for the PM-ISE to communicate the progress of the ISE to Congress and other stakeholders. The ISE P&I Integration Program provides the information the PM-ISE needs to advocate for funding and management attention for specific ISE programs and activities. By blending fact-based performance and investment data along with a working knowledge of their programs' achievements and needs, the PM-ISE will compile a holistic view of achievements to date and still outstanding needs in the ISE Maturity Score Card. The Score Card offers a means for the PM-ISE to communicate externally the progress of the ISE. Figure 13 shows a notional version of the Maturity Score Card that will be used in future reporting of ISE progress.

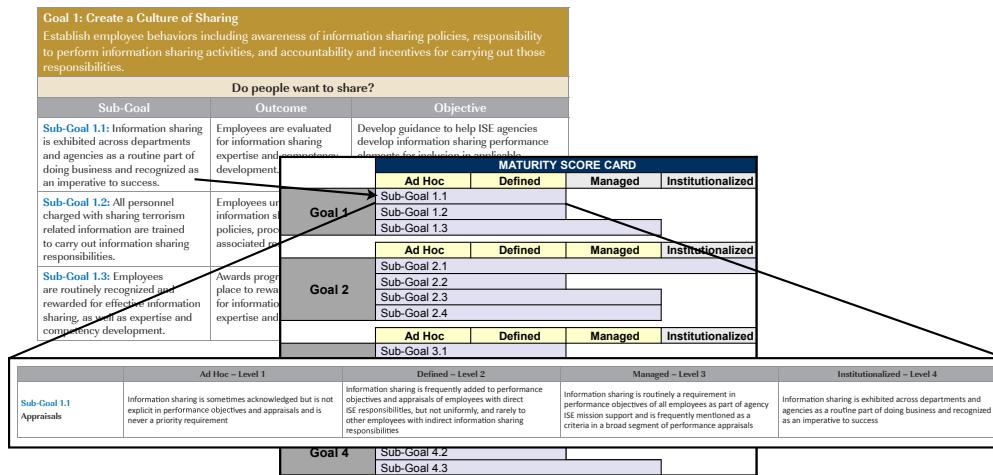


Figure 13. Connecting Sub-Goals and Maturity Model to a Notional Maturity Score Card

In summary, the ISE Framework, the ISE Maturity Model, the P&I process, and the ISE Maturity Score Card together provide the tools and techniques needed to ensure that ISE resources are applied to those ISE programs that address the highest priority goals and sub-goals and that meet established performance goals and targets.

APPENDICES

APPENDIX A – ISE FRAMEWORK

1

GOAL

| Goal 1: Create a Culture of Sharing | | |
|--|--|--|
| Establish employee behaviors including awareness of information sharing policies, responsibility to perform information sharing activities, and accountability and incentives for carrying out those responsibilities. | | |
| Do people want to share? | | |
| Sub-Goal | Outcome | Objective |
| Sub-Goal 1.1: Information sharing is exhibited across departments and agencies as a routine part of doing business and recognized as an imperative to success. | Employees are evaluated for information sharing expertise and competency development. | Develop guidance to help ISE agencies develop information sharing performance elements for inclusion in applicable employee performance appraisals. |
| Sub-Goal 1.2: All personnel charged with sharing terrorism related information are trained to carry out information sharing responsibilities. | Employees understand information sharing policies, processes, and associated responsibilities. | Develop ISE Core Awareness Training Course to help move federal agencies from the traditional “need to know” culture to a “responsibility to provide.” |
| Sub-Goal 1.3: Employees are routinely recognized and rewarded for effective information sharing, as well as expertise and competency development. | Awards programs are put in place to reward employees for information sharing expertise and competency. | Put awards programs in place that reward employees for information sharing expertise and competency. |

2
GOAL

| Goal 2: Reduce Barriers to Sharing Use of Policy, Business Process and Practices, and Technology to remove obstacles and enable information sharing. | | |
|---|---|---|
| Are there impediments to sharing? | | |
| Sub-Goal | Outcome | Objective |
| Sub-Goal 2.1: Federal Departments and Agencies practice security reciprocity among Federal, State, Local, and Private Sector entities, to include people, facilities, and systems. | Security policy program in place for State and Local partners. | <ul style="list-style-type: none"> • Develop interagency policy recommendations for a centralized management framework to coordinate the access to and protection of classified information when shared with SLT partners. • Implement the centralized security management framework in all Federal agencies, creating uniformity and clarity for SLT partners. |
| | Harmonized Federal information systems security technical standards support reciprocity across all groups and organizations | <ul style="list-style-type: none"> • Update existing laws, policies, and standards to adopt a single Federal baseline for IT systems security and to support reciprocity. |
| Sub-Goal 2.2: Consistent marking and handling of controlled unclassified information across the U.S. Government; practices also adopted by SLT and Private sector. | Enable consistent handling and sharing of CUI at all levels of government. | <ul style="list-style-type: none"> • Implement, with CUI Office oversight, unified CUI policies in accordance with the CUI Registry including safeguarding, dissemination, marking, dispute resolution, and designation. • Implement centralized and agency-specific training for CUI Framework. • Identify resources for technology and personnel to support agencies' transition from the current SBU regime to the CUI Framework. |
| | Non-Federal participants understand how to implement the CUI framework. | <ul style="list-style-type: none"> • Provide guidance to non-Federal partners on how to implement the CUI Framework. • Provide guidance to non-Federal partners on how to implement training for CUI Framework. |
| Sub-Goal 2.3: ISE participants build trusted distributed infrastructure for sharing information with all other participants, and are able to leverage repeatable processes from each other's Architecture programs to maximize availability of common ISE shared services. | Information is accessible across trusted enclaves [trusted enclaves and trusted interconnects]. | <ul style="list-style-type: none"> • Implement ISE systems using common technical standards. • Implement ISE Shared Spaces to support mission business processes and associated information. • Fully implement processes for reciprocal acceptance and verification of IT systems security for Federal, State, local, and private sector partners. |

2
GOAL

| Goal 2: Reduce Barriers to Sharing | | |
|---|---|--|
| Use of Policy, Business Process and Practices, and Technology to remove obstacles and enable information sharing. | | |
| Are there impediments to sharing? | | |
| Sub-Goal | Outcome | Objective |
| Sub-Goal 2.4: ISE Departments and Agencies, SLT, and the private sector protect privacy in a consistent manner | Federal agencies have a written ISE privacy policy. | <ul style="list-style-type: none"> • Adopt an ISE privacy protection policy. |
| | Federal agencies have implemented the written ISE privacy policy. | <ul style="list-style-type: none"> • Apply ISE privacy protection policy to ISE information sharing systems and arrangements. |
| | SLT partners have privacy policies that are at least as comprehensive as the ISE privacy guidelines. | <ul style="list-style-type: none"> • Implement privacy policies that incorporates ISE requirements. |
| | Private Sector partners have privacy policies that are at least as comprehensive as the ISE privacy guidelines. | <ul style="list-style-type: none"> • Implement privacy policies that incorporate ISE requirements. |
| | Fusion centers safeguard privacy and civil liberties. | <ul style="list-style-type: none"> • Establish processes for drafting and updating privacy policies at State and major urban area fusion centers. |

3
GOAL

Goal 3: Improve sharing practices with federal, state, local, tribal and foreign partners
Enhance information sharing by standardizing practices, improving interagency coordination, and developing guidance and enabling infrastructure to support the information sharing mission.

| What practices should we create or improve to promote sharing? | | |
|--|--|--|
| Sub-Goal | Outcome | Objective |
| <p>Sub-Goal 3.1: Federal, State, Local and Tribal authorities establish or improve their ability to recognize, gather, document, evaluate and share information regarding suspicious activities and incidents.</p> | <p>State and major area fusion centers and localities have been fully incorporated into a Nationwide SAR process.</p> | <ul style="list-style-type: none"> Put in place policies and procedures for handling SAR, including privacy and civil liberties protections, at State and major urban area fusion centers and local law enforcement agencies. Train executives, analysts and front line officers at State and major area fusion centers and local law enforcement agencies in the NSI process. Fully implement processes for gathering, analyzing, and sharing ISE-SAR information at State and major urban area fusion centers and local law enforcement agencies. |
| | <p>Federal agencies improve the gathering and sharing of ISE SARs.</p> | <ul style="list-style-type: none"> Put in place policies and procedures for handling SAR including privacy and civil liberties protections at Federal agencies. Fully implement processes for gathering, analyzing, and sharing ISE-SAR information at Federal agencies. |
| <p>Sub-Goal 3.2: A national, integrated network of state and major urban area fusion centers that enables Federal and SLT and PS organizations to gather, document, process, analyze, and share relevant information in order to protect our communities.</p> | <p>State and local authorities are better informed because they access classified and unclassified reports regarding tactics, techniques and procedures used by adversaries.</p> | <ul style="list-style-type: none"> Develop and disseminate Federal government products that inform the NSI process to state and/or major urban area fusion centers. Access Federal products at State and major urban area fusion centers to inform the SAR process. Establish risk assessment processes at State and major urban area fusion centers to develop Priority Information Needs (PINs). Use Priority Information Needs (PINs) to inform the development of training programs for frontline officers and analysts. |
| | <p>Sustained support for fusion centers (to include personnel, systems, etc).</p> | <ul style="list-style-type: none"> Establish sustainability task force. Develop sustainment strategy. Establish joint fusion center program office. Develop and institutionalize a process to mitigate gaps in fusion center capabilities identified as part of baseline capability assessments. |
| | <p>Baseline capabilities achieved at Fusion centers.</p> | <ul style="list-style-type: none"> Develop and institutionalize a process for assessing baseline capabilities. Develop and institutionalize a process to mitigate gaps in fusion center capabilities identified as part of baseline capability assessments. |

| Goal 3: Improve sharing practices with federal, state, local, tribal and foreign partners Enhance information sharing by standardizing practices, improving interagency coordination, and developing guidance and enabling infrastructure to support the information sharing mission. | | |
|---|--|---|
| What practices should we create or improve to promote sharing? | | |
| Sub-Goal | Outcome | Objective |
| Sub-Goal 3.2: (continued) | State, local, and Federal Departments and Agencies are better able to protect our local communities. | <ul style="list-style-type: none"> Federal agencies use ISE SARs as part of investigative and other law enforcement and homeland security related efforts. Generate Analytic products as a result of pattern and trend analysis of SARs. Identify new individuals or groups involved in terrorism-related crimes based on SAR analysis. Dismantle or disrupt terrorist groups based on SAR analysis. Initiate Investigations as a result of ISE-SARs. Initiate investigations as a result of ISE-SARs that result in arrests, convictions, or other law enforcement actions. Enhance preparedness planning based on ISE-SAR-related threat analysis. Enhance critical infrastructure protection based on ISE-SAR-related threat analysis. |
| Sub-Goal 3.3: Federal agencies produce, share and disseminate both time-sensitive and strategic information and intelligence products that meet SLTP needs | Further enable the production and dissemination of clear, tailored, relevant, official and federally-coordinated threat information in a timely, consistent and usable manner. | <ul style="list-style-type: none"> Make ITACG Fully Functional. |
| | Information dissemination from Federal agencies to fusion centers and from fusion centers to State and local agencies is improved. | <ul style="list-style-type: none"> Provide SLT personnel direct access to classified systems. Coordinate the production and dissemination of unclassified and classified products. Train personnel at fusion centers to access Federal products and information via unclassified and classified networks. Coordinate dissemination of alerts, warnings and notifications. |
| Sub-Goal 3.4: Federal departments and agencies have implemented appropriate policies and processes to coordinate and facilitate the sharing of information with foreign governments and allies. | The ISE supports and facilitates appropriate information sharing between executive departments and agencies and foreign partners and allies. | |

4 COAL

| Goal 4: Institutionalize Sharing Make information sharing routine through championing, leading, using and sustaining efforts to standardize policies, resources, business practices, and technologies. | | |
|---|--|---|
| Have we formalized (documented and approved) information sharing as a routine function of a mission? | | |
| Sub Goal | Outcome | Objective |
| Sub-Goal 4.1: Integrated performance and investment process monitors progress toward performance goals and successfully uses investments to support activities that maintain or enhance information sharing. | ISE priorities are integrated into Department's and Agency's investment and performance management structures and processes. | <ul style="list-style-type: none"> • Affect federal budget guidance. • Include ISE Programs in agency investment planning. • Monitor ISE program performance. |
| Sub-Goal 4.2: ISE participants sustain their investments in information systems that support a trusted, distributed infrastructure for sharing information. | ISE architecture principles are integrated into participants' capital investment planning processes for information systems. | <ul style="list-style-type: none"> • Apply ISE architecture principles to agency enterprise and segment architectures. • Integrate architectures into agency investment processes. |
| | ISE participants improve the information sharing performance of their systems. | <ul style="list-style-type: none"> • Measure information sharing performance of ISE systems as part of OMB Exhibit 300 submission process. |
| | Vendors adopt ISE standards into products. | <ul style="list-style-type: none"> • Incorporate hardware and software products into ISE participants' systems that support ISE standards (Technical and Functional Standards). |
| | Reconcile interoperability and interconnectivity problems between SBU networks, portals, and systems that share information with Federal departments and agencies, SLT governments and the private sector. | <ul style="list-style-type: none"> • Ensure ISE participants' SBU systems and infrastructure are interoperable and interconnect across the ISE. |
| Sub-Goal 4.3: ISE participants use common practices and policies for producing, handling, and using information. | ISE participants prepare terrorism-related information for maximum distribution and access across the ISE. | <ul style="list-style-type: none"> • Incorporate hardware and software products into ISE participants' systems that support ISE standards (Technical and Functional Standards). • Ensure ISE participants' SBU systems and infrastructures are interoperable and interconnect across the ISE. |

APPENDIX B – DETAILED 2008-2009 ISE PERFORMANCE RESULTS

Background

The PM-ISE performance management approach has evolved as the ISE has matured over time. Focused initially on measuring progress toward implementing the ISE—adoption of new or improved policies, business processes, architectures, standards, and systems—the approach has now begun to incorporate concrete indicators of information sharing progress in operational situations, for example sharing of suspicious activity reports. The adoption of the ISE Framework, which includes the context for determining the elements to be measured within the ISE, provides the foundation for a performance scorecard that embodies both ISE implementation progress and operational information sharing performance.

Annual performance goals, responding to specific direction in IRTPA, are used to measure progress in institutionalizing ISE capabilities as well as to guide the further development and performance of the ISE.⁴¹ The performance goals adopted in last year's report continue to provide a target level of performance against which actual achievement can be compared in the context of the four goals that make up the ISE Framework.⁴² The 2009 performance goals were adopted prior to the development of the ISE Framework. Consequently, although the majority of them align closely with the Framework, there are exceptions. For example, Privacy and Civil Liberties Protection was included under Goal 1 in last year's annual report, but is part of Goal 2 in the new ISE Framework. For continuity, this section will discuss the performance goals as they were presented in last year's report. In future reports, all performance results will be directly traceable to the goals and sub-goals in the ISE framework.

Methodology and Scope

ISE performance measures provide the PM-ISE and the stakeholders with data to make fact-based decisions and hold agencies accountable for the ISE's evolution. The first steps, accomplished largely through the ISE Framework, are to determine which items to measure and document intended outcomes. These outcomes are used to generate performance goals, targets, and measures of both ISE implementation progress and operational information sharing performance which, in turn, drive agency implementation and data gathering efforts.

The PM-ISE conducts a biannual assessment of ISC-member agencies to gauge progress in implementing the ISE. The data included here represent a close-out of the full 2009 Performance Cycle following the spring data collection in April 2009 and is organized according to the table below.

⁴¹ IRTPA (as amended) §1016(h)(2)(A) and (B).

⁴² Annual Report to the Congress on the Information Sharing Environment (June 2008), pp. 51-52.

| 2009 ISE Metric Objectives |
|---|
| <p>To further create a culture of sharing, agencies will:</p> <ol style="list-style-type: none"> 1. Ensure all personnel charged with sharing terrorism information complete ISE awareness training. 2. Make information sharing a factor in awards and incentives programs. 3. Add information sharing elements to employee performance appraisals. 4. Complete Stage 1 of the ISE Privacy and Civil Liberties Implementation Manual. |
| <p>To further reduce barriers to sharing, agencies will:</p> <ol style="list-style-type: none"> 5. Implement ISE Shared Spaces. 6. Begin to adopt the Controlled Unclassified Information (CUI) Framework. 7. Work toward security reciprocity among Federal/State/local and private sector entities, to include people facilities and systems. |
| <p>To improve sharing practices with Federal, State, local, tribal and foreign partners, agencies will:</p> <ol style="list-style-type: none"> 8. Make the ITACG fully-functional. 9. Increase fusion centers' access to terrorism-related information and ISE capabilities. 10. Make available to the appropriate personnel tools and mechanisms for the negotiation of terrorism-related agreements and arrangements. 11. Complete initial efforts to establish a national process for suspicious activity reporting. |
| <p>To institutionalize sharing, agencies will:</p> <ol style="list-style-type: none"> 12. Further integrate their IT management structures with ISE Enterprise Architecture principles. 13. Adopt ISE standards. 14. Further integrate ISE investment and performance management initiatives into department and agency management structures through out-year planning and increased involvement of Performance Improvement Officers. |

FY 2010 Performance Goals

Each year, the PM-ISE must establish or modify annual performance goals for the following year, to chart a course for ISC-member agencies in implementing the ISE and reporting those results to Congress.⁴³ Performance goals for 2010 will be directly tied to the goals and sub-goals in the ISE Framework. Since the ISE framework has been completed, however, and because some of the activities and products that will support the Framework are still under development, it is premature to identify specific performance goals at this time. Instead The PM-ISE will incorporate performance goals, measures, and targets into the Framework over the next several months and use those to drive regular assessments of ISE performance over the next year.

⁴³ IRTPA (as amended) §1016(h)(2)(B).

GOAL 1: CREATE A CULTURE OF SHARING

1
GOAL

1. ISE Awareness Training

| | | | |
|------------------------------|--|---------------|----------------------|
| Measurement Objective | Ensure all personnel charged with sharing terrorism information complete ISE awareness training. | | |
| 2009 Metric | 10 out of 15 ISE Departments and Agencies have a plan for implementing ISE Guidance 104 guidance on Information Sharing Environment Core Awareness Training. | | |
| Agency | 2009 Response | Agency | 2009 Response |
| CIA | Yes | DOJ | Yes |
| DHS | Yes | DoS | Under Development |
| DNI | Yes | DOT | Yes |
| DOC | Yes | FBI | Yes |
| DoD/JCS | Yes | HHS | No |
| DOE | No | NCTC | No |
| DOI | Yes | Treasury | No |
| 2009 Highlight | As of April 2009, 10 of 15 ISE Departments and Agencies indicated that they had implemented the ISE Core Awareness Training. | | |

2. Incentives for Information Sharing

| | | | |
|------------------------------|--|---------------|----------------------|
| Measurement Objective | Make information sharing a factor in awards and incentives programs | | |
| 2009 Metric | 11 out of 15 ISE Departments and Agencies have adopted (or intend to adopt) affirmative incentives for information sharing. | | |
| Agency | 2009 Response | Agency | 2009 Response |
| CIA | Yes | DOJ | Yes |
| DHS | Under Development | DoS | Under Development |
| DNI | Yes | DOT | Yes |
| DOC | No | FBI | No |
| DoD/JCS | Yes | HHS | Yes |
| DOE | No | NCTC | No |
| DOI | Yes | Treasury | Yes |
| 2009 Highlight | 11 out of 15 ISE Departments and Agencies have adopted or intend to adopt incentives such as personnel recognition, cash awards, and other rewards. This signals that 10 agencies have now adopted incentives, one agency is developing them, and four have taken no action. | | |

1
GOAL

3. Personnel Appraisals

| | | | | |
|------------------------------|---|---------------|----------------------|--|
| Measurement Objective | Add information sharing elements to employee performance appraisals. | | | |
| 2009 Metric | 13 out of 15 ISE Departments and Agencies have distributed (or intend to distribute) guidance for incorporating information sharing elements in performance appraisals. | | | |
| Agency | 2009 Response | Agency | 2009 Response | |
| CIA | Yes | DOJ | Yes | |
| DHS | Under Development | DoS | Yes | |
| DNI | Yes | DOT | Yes | |
| DOC | No | FBI | Yes | |
| DoD/JCS | Under Development | HHS | No | |
| DOE | Under Development | NCTC | Yes | |
| DOI | Under Development | Treasury | Yes | |
| 2009 Highlight | Eight agencies have already implemented new appraisals, while four have partially implemented, and one is awaiting approval to implement in October 2009 | | | |

4. Privacy Policies

| | | | | |
|------------------------------|--|---------------|----------------------|--|
| Measurement Objective | Complete Stage 1 of the ISE Privacy and Civil Liberties Implementation Manual. | | | |
| 2009 Metric | 12 out of 15 ISE Departments and Agencies are developing a written ISE privacy protection policy, as required by ISE Privacy Guidelines, Section 12(d). | | | |
| Agency | 2009 Response | Agency | 2009 Response | |
| CIA | Under Development | DOJ | Under Development | |
| DHS | Yes | DoS | Under Development | |
| DNI | Under Development | DOT | No | |
| DOC | No | FBI | Yes | |
| DoD/JCS | Under Development | HHS | No | |
| DOE | Under Development | NCTC | Under Development | |
| DOI | Under Development | Treasury | Under Development | |
| 2009 Highlight | Each agency is required to provide the Privacy Guidelines Committee with a copy of its written ISE privacy policy. Only two agencies have completed their policy, while ten additional agencies have drafted privacy policies, with several being in the approval stages. | | | |

GOAL 2: REDUCE BARRIERS TO SHARING

2

GOAL

5. ISE Shared Spaces

| | | | | |
|------------------------------|--|---------------|----------------------|--|
| Measurement Objective | Implement ISE Shared Spaces. | | | |
| 2009 Metric | 2 out of 3 required ISE Departments and Agencies participating in the SAR Evaluation Environment have implemented ISE Shared Spaces as it relates to SAR. | | | |
| Agency | 2009 Response | Agency | 2009 Response | |
| CIA | Not Applicable | DOJ | Not Applicable | |
| DHS | Under Development | DoS | Not Applicable | |
| DNI | Not Applicable | DOT | Not Applicable | |
| DOC | Not Applicable | FBI | Yes | |
| DoD/JCS | Yes | HHS | Not Applicable | |
| DOE | Not Applicable | NCTC | Not Applicable | |
| DOI | Not Applicable | Treasury | Not Applicable | |
| 2009 Highlight | As of spring 2009, 2 out of 3 required ISE Departments and Agencies participating in the SAR Evaluation Environment have implemented ISE Shared Spaces. At least one agency (DHS) is continuing to improve upon its initial capability by conducting an intradepartmental pilot to implement a shared space for SAR. | | | |

6. CUI Framework – See Part Two for information on progress

7. Personnel, Facilities, and Systems Security Practices

7a. Personnel Security Reciprocity:

| | | | | |
|------------------------------|---|---------------|----------------------|--|
| Measurement Objective | Work toward security reciprocity among Federal/State/local and private sector entities, to include people facilities and systems. | | | |
| 2009 Metric | 14 out of 15 ISE Departments and Agencies recognize background investigations and adjudications completed by another agency. | | | |
| Agency | 2009 Response | Agency | 2009 Response | |
| CIA | Yes | DOJ | Yes | |
| DHS | No | DoS | Yes | |
| DNI | Yes | DOT | Yes | |
| DOC | Yes | FBI | Yes | |
| DoD/JCS | Yes | HHS | Yes | |
| DOE | Yes | NCTC | Yes | |
| DOI | Yes | Treasury | Yes | |

2
GOAL

7b. Facilities Security Reciprocity:

| | | | |
|------------------------------|---|---------------|----------------------|
| Measurement Objective | Work toward security reciprocity among Federal/State/local and private sector entities, to include people facilities and systems. | | |
| 2009 Metric | 12 out of 15 ISE Departments and Agencies recognize other agencies' facilities accreditation processes. | | |
| Agency | 2009 Response | Agency | 2009 Response |
| CIA | Yes | DOJ | No Reply |
| DHS | Yes | DoS | Yes |
| DNI | Yes | DOT | Yes |
| DOC | Not Applicable | FBI | Yes |
| DoD/JCS | Yes | HHS | Yes |
| DOE | Yes | NCTC | Not Applicable |
| DOI | Yes | Treasury | Yes |

7c. IC Systems/IT Security Reciprocity:

| | | | |
|------------------------------|---|---------------|----------------------|
| Measurement Objective | Work toward security reciprocity among Federal/State/local and private sector entities, to include people facilities and systems. | | |
| 2009 Metric | 11 out of 15 ISE Departments and Agencies accept IC "certification of a system or other item of IT." | | |
| Agency | 2009 Response | Agency | 2009 Response |
| CIA | Yes | DOJ | Not Applicable |
| DHS | Yes | DoS | Yes |
| DNI | Yes | DOT | No |
| DOC | Not Applicable | FBI | No |
| DoD/JCS | Yes | HHS | Yes |
| DOE | Yes | NCTC | Yes |
| DOI | Yes | Treasury | Yes |

7d. Non-IC Systems/IT Security Reciprocity:

| | | | |
|------------------------------|---|---------------|----------------------|
| Measurement Objective | Work toward security reciprocity among Federal/State/local and private sector entities, to include people facilities and systems. | | |
| 2009 Metric | 11 out of 15 ISE Departments and Agencies accept non-IC "certification of a system or other item of IT." | | |
| Agency | 2009 Response | Agency | 2009 Response |
| CIA | Yes | DOJ | Yes |
| DHS | Yes | DoS | Yes |
| DNI | Yes | DOT | No |
| DOC | Not Applicable | FBI | No |
| DoD/JCS | Yes | HHS | No |
| DOE | Yes | NCTC | Yes |
| DOI | Yes | Treasury | Yes |

| | |
|-----------------------|---|
| 2009 Highlight | 14 out of 15 ISE Departments and Agencies now recognize background investigations and adjudications completed by another agency; 80% recognize other agencies' facilities accreditation processes; 73% accept at least one IC certification; and 73% accepted a non-IC certification of at least one system, demonstrating progress in meeting Congressional and Executive branch security reciprocity goals. |
|-----------------------|---|

GOAL 3: IMPROVE SHARING PRACTICES WITH FEDERAL, STATE, LOCAL, TRIBAL AND FOREIGN PARTNERS

3
GOAL

- 8. ITACG – See Part Two for information on progress
- 9. State and Major Urban Area Fusion Centers – See Part Two for information on progress
- 10. Information Sharing with Foreign Partners

| | | | |
|------------------------------|---|---------------|----------------------|
| Measurement Objective | Make available to the appropriate personnel tools and mechanisms for the negotiation of terrorism-related agreements and arrangements. | | |
| 2009 Metric | 3 out of 15 ISE Departments and Agencies have used the Checklist of Issues for Negotiating Terrorism Information Sharing Agreements and Arrangements. | | |
| Agency | 2009 Response | Agency | 2009 Response |
| CIA | Not Applicable | DOJ | Yes |
| DHS | No Reply | DoS | Yes |
| DNI | No | DOT | No |
| DOC | Not Applicable | FBI | No |
| DoD/JCS | Under Development | HHS | No |
| DOE | Yes | NCTC | Not Applicable |
| DOI | Not Applicable | Treasury | No |
| 2009 Highlight | The Foreign Government Information Sharing Working Group issued a recommended checklist of issues for agencies to consider when negotiating terrorism-related information sharing agreements with foreign partners, including privacy protections and possible review procedures. As of spring 2009, 3 out of 15 ISE Departments and Agencies were using the checklist. This data reflects only departments and agencies that have foreign sharing relationships. | | |

- 11. SAR Process – See Part Two for information on progress

4 GOAL

GOAL 4: INSTITUTIONALIZE SHARING

12. Enterprise Architecture

| | | | |
|------------------------------|--|---------------|----------------------|
| Measurement Objective | Further integrate their IT management structures with ISE Enterprise Architecture principles. | | |
| 2009 Metric | 13 out of 15 ISE Departments and Agencies have incorporated (or intend to incorporate) ISE EAF and ISE PAIS into their Information Sharing Segment Architecture or agency's enterprise architecture. | | |
| Agency | 2009 Response | Agency | 2009 Response |
| CIA | Yes | DOJ | Yes |
| DHS | Yes | DoS | Under Development |
| DNI | Yes | DOT | Under Development |
| DOC | Not Applicable | FBI | Under Development |
| DoD/JCS | Yes | HHS | No |
| DOE | Under Development | NCTC | Yes |
| DOI | Under Development | Treasury | Under Development |
| 2009 Highlight | This number reflects seven agencies who have already incorporated, and another six who have plans to incorporate the principles in their agencies' architecture. | | |

13. Common Terrorism Information Sharing Standards (CTISS)

13a. ISE-G-106 Technical Standard:

| | | | |
|------------------------------|---|---------------|----------------------|
| Measurement Objective | Adopt ISE standards. | | |
| 2009 Metric | 5 out of 15 ISE Departments and Agencies incorporated the ISE-G-106 Technical Standard Information Assurance, Version 1.0 standards into their Department/Agency level information systems and current and future planning. | | |
| Agency | 2009 Response | Agency | 2009 Response |
| CIA | No Reply | DOJ | Yes |
| DHS | Yes | DoS | No |
| DNI | Under Development | DOT | No |
| DOC | Not Applicable | FBI | No |
| DoD/JCS | Yes | HHS | No |
| DOE | No | NCTC | See DNI |
| DOI | Yes | Treasury | Under Development |

13b. ISE-G-107 Technical Standard:

| | | | |
|------------------------------|---|---------------|----------------------|
| Measurement Objective | Adopt ISE standards. | | |
| 2009 Metric | 5 out of 15 ISE Departments and Agencies have incorporated the ISE-G-107 Technical Standard Core Transport, Version 1.0 standards into their Department/Agency level information systems and current and future planning. | | |
| Agency | 2009 Response | Agency | 2009 Response |
| CIA | No Reply | DOJ | Yes |
| DHS | Yes | DoS | No |
| DNI | Under Development | DOT | No |
| DOC | Not Applicable | FBI | Yes |
| DoD/JCS | Yes | HHS | No |
| DOE | No | NCTC | See DNI |
| DOI | No | Treasury | Under Development |

13c. ISE-G-108 Identity and Access Management Framework for the ISE:

| | | | |
|------------------------------|---|---------------|----------------------|
| Measurement Objective | Adopt ISE standards. | | |
| 2009 Metric | 2 out of 15 ISE Departments and Agencies have implemented the ISE-G-108 Identity and Access Management Framework for the ISE. | | |
| Agency | 2009 Response | Agency | 2009 Response |
| CIA | Under Development | DOJ | Yes |
| DHS | Yes | DoS | No |
| DNI | Under Development | DOT | No |
| DOC | Not Applicable | FBI | No |
| DoD/JCS | Under Development | HHS | No |
| DOE | No | NCTC | See DNI |
| DOI | No | Treasury | No |

| | |
|-----------------------|--|
| 2009 Highlight | <p>Agencies cited the National Information Exchange Model (NIEM) and FEA Standards as examples of where they are working across the ISE to align technologies to facilitate information access and exchange.</p> <p>PM-ISE released a series of technical standards, including Information Assurance, Core Transport, and Identity and Access Management (IdAM). The data revealed that 5 out of 15 ISE Departments and Agencies reported adoption of the Information Assurance standard, 5 out of 15 have incorporated the Core Transport standard, and 2 out of 15 have implemented the IdAM standard.</p> |
|-----------------------|--|

4 GOAL

14. Investment and Performance Integration

| | | | | |
|------------------------------|--|----------------------|----------|----------------------|
| Measurement Objective | Further integrate ISE investment and performance management initiatives into department and agency management structures through out-year planning and increased involvement of Performance Improvement Officers. | | | |
| 2009 Metric | 9 out of 15 ISE Departments and Agencies apply transition plans and relevant Segment Architecture transition plans at key decision points in the IT capital planning and investment cycle. | | | |
| | Agency | 2009 Response | | 2009 Response |
| | CIA | Not Applicable | DOJ | Yes |
| | DHS | Yes | DoS | Yes |
| | DNI | Yes | DOT | Yes |
| | DOC | Not Applicable | FBI | No |
| | DoD/JCS | Yes | HHS | No |
| | DOE | No | NCTC | No Reply |
| | DOI | Yes | Treasury | Yes |
| 2009 Highlight | One approach to measuring how well an agency is linking performance and investment is to identify points in the investment cycle where individuals consider the enterprise architecture in investment decisions. As of spring 2009, 7 out of 15 ISE Departments and Agencies had demonstrated that they have applied enterprise architecture transition plans at key decision points in their IT investment cycle. | | | |

APPENDIX C – ACRONYMS AND ABBREVIATIONS

| | |
|--------|--|
| AWN | Alerts, Warnings, and Notifications |
| BJA | Bureau of Justice Assistance |
| CBP | Customs and Border Protection |
| CDWG | Classified Domain Sub-Working Group |
| CIA | Central Intelligence Agency |
| CIO | Chief Information Officer |
| CONOPS | Concept of Operations |
| CT | Counterterrorism |
| CTISS | Common Terrorism Information Sharing Standards |
| CUI | Controlled Unclassified Information |
| DHS | Department of Homeland Security |
| DNI | Director of National Intelligence |
| DOC | Department of Commerce |
| DoD | Department of Defense |
| DOI | Department of the Interior |
| DOJ | Department of Justice |
| DoS | Department of State |
| DOT | Department of Transportation |
| EA | Enterprise Architecture |
| EAF | Enterprise Architecture Framework |
| EE | Evaluation Environment |
| FBI | Federal Bureau of Investigation |
| FBINet | FBI Secret Domain Network |
| FEA | Federal Enterprise Architecture |
| FIRES | Foreign Intelligence Relationship Enterprise System |
| FSAM | Federal Segment Architecture Methodology |
| FY | Fiscal Year |
| GAO | Government Accountability Office |
| HS | Homeland Security |
| HSDN | Homeland Security Data Network |
| IC | Intelligence Community |
| ICAM | Identity, Credential, and Access Management |
| ICE | Immigration and Customs Enforcement |
| IdAM | Identity and Access Management |
| IRTPA | Intelligence Reform and Terrorism Prevention Act of 2004 |

| | |
|---------|---|
| ISC | Information Sharing Council |
| ISE | Information Sharing Environment |
| ISE EAF | Information Sharing Environment Enterprise Architecture Framework |
| IT | Information Technology |
| ITACG | Interagency Threat Assessment and Coordination Group |
| JTTF | Joint Terrorism Task Force |
| LAPD | Los Angeles Police Department |
| LEISS | Law Enforcement Information Sharing Service |
| MPD | Metropolitan Police Department (Washington D.C.) |
| NARA | National Archives and Records Administration |
| NCTC | National Counterterrorism Center |
| NFCCG | National Fusion Center Coordination Group |
| NIEM | National Information Exchange Model |
| NOL-S | NCTC Online-Secret |
| NRC | Nuclear Regulatory Commission |
| NSI | Nationwide SAR Initiative |
| NSIS | National Strategy for Information Sharing |
| NSS | National Security Systems |
| ODNI | Office of the Director of National Intelligence |
| OMB | Office of Management and Budget |
| OPM | Office of Personnel Management |
| PAIS | Profile and Architecture Implementation Strategy |
| PGC | Privacy Guidelines Committee |
| PIO | Performance Improvement Officer |
| P&I | Performance and Investment |
| PM-ISE | Program Manager, Information Sharing Environment |
| SAR | Suspicious Activity Reporting |
| SBU | Sensitive But Unclassified |
| SLT | State, Local, and Tribal |
| TIPS | Terrorism Information Sharing Products |
| TSC | Terrorist Screening Center |
| TWPDES | Terrorist Watchlist Person Data Exchange Standard |

ISE

PROGRAM MANAGER, INFORMATION SHARING ENVIRONMENT
WASHINGTON, D.C. 20511

202.331.2490

VISIT US ON THE WEB AT [HTTP://WWW.ISE.GOV](http://www.ise.gov)

